FUJITSU

SERVIS™ IP-Serial コンソールスイッチ

インストール / 管理 / ユーザーガイド

USA Notification

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Safety and EMC Approvals and Markings

UL, FCC Class A, cUL, ICES-003, CE, ACA (C-Tick), CB, VCCI-A, MIC/RRL, GS, GOST

Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

SERVIS™ IP-Serial コンソールスイッチ

インストール / 管理 / ユーザーガイド

注意

この記号は、装置に付属のマニュアル類に操作およびメンテナンス (サービス) に関する重要な注意事項が機材されていることをユーザーに警告するものです。

危険電圧

この記号は、感電の危険性がある絶縁されていない危険電圧が製品のエンクロージャ内に存在することをユーザーに警告するものです。

電源オン

この記号は、主電源スイッチがオンになっていることを示します。

電源オフ

この記号は、主電源スイッチがオフになっていることを示します。

保護接地端子

この記号は、装置にほかの接続を行う前に、まず端子を設置接続する必要があることを示します。

目次

図目次

表目次

章

1

はじめに

SERVIS IP-Serial コンソールスイッチ (以降、コンソールスイッチと略します。) は、ターゲットデバイスのコンソール、モデム、電源デバイスなど、接続されたデバイスへのアクセスおよびその管理のための単一ポイントとして機能する 1U アプライアンスです。コンソールスイッチは、セキュアなリモートデータセンター管理、および世界中のあらゆる場所からの IT 資産の帯域外管理をサポートしています。

コンソールスイッチは、セキュアなローカル (CONSOLE ポート) およびリモート (IP およびダイヤルアップ) アクセスを提供します。コンソールスイッチは、フラッシュメモリ内の永続的なファイルシステムを使用して Linux® オペレーティングシステムを実行し、FTP サーバーあるいは MergePoint Access 管理ソフトウェアサーバーからアップグレードさせることができます。

1 つのコンソールスイッチに複数の管理者が同時にログインすることができ、コンソールスイッチへのアクセスおよび設定のために Web マネージャ、コマンドラインインターフェイス (CLI ユーティリティ) 、あるいは MergePoint Access ソフトウェアを使用して実行することができます。

2 つの PC カード / スロットは、モデム (V.92 およびワイヤレス GSM/CDMA) 、Ethernet、高速 Ethernet (光ファイバー) およびストレージ PC カード (16 ビットと 32 ビット) に対応しています。1 つの USB ポートは、モデム (V.92 およびワイヤレス GSM/CDMA) 、ストレージデバイス、および USB ハブに対応しています。2 つの高速 Ethernet ポートは、冗長性やより高い信頼性を実現するために、複数のネットワークへの接続や Ethernet 結合 (フェイルオーバー) の設定に対応しています。PPP (Point-to-Point Protocol) を使用したダイヤルインおよびセキュアなダイヤルバックを行う場合は、外部のモデムまたはワイヤレスのモデム CardBus デバイスを使用できます。

特長と利点

アクセスオプション

次のローカル (アナログ CONSOLE ポート) およびリモート (デジタル IP およびダイヤルアップ) のオプションを使用して安全にアクセスすることができます。

- LAN/WAN IP ネットワーク接続

- シリアルポートまたは AUX ポート、あるいは PC カードスロットの 1 つ または USB ポートに取り付けてある PC フォンカード（モデム、GSM あるいは CDMA）に接続したモデムへの接続。
- ターゲットデバイス接続。承認ユーザーは Web マネージャを使用してターゲットデバイスに対して Telnet、SSHv1、または SSHv2 接続を確立できます。Telnet または SSH を使用してターゲットデバイス接続を行う場合、セキュリティプロファイルの設定で Telnet サービスまたは SSH サービスが有効になっている必要があります。
- コンソールスイッチ コンソール接続。管理者は、ローカル端末から、またはコンソールポートに接続した端末エミュレーションプログラムがあるコンピュータからログインし、CLI ユーティリティを使用できます。ログイン時に CLI ユーティリティのプロンプト (--|- cli>) が表示されます。

複数の管理者がコンソールスイッチにログインし、アクティブな CLI セッションまたは Web マネージャセッションを行うことができます。別の管理者またはシステムによって設定が変更された場合は、すべてのセッションに すべてのセッションに「アプライアンス設定にセッション外から変更が加えられています。」という警告メッセージが送信されます。このメッセージを受け取った場合、各管理者はセッション中に行った変更が保存されていることを確認する必要があります。

Web マネージャ

ユーザーおよび管理者は、HTTP または HTTPS によってアクセスする Web マネージャを使用してほとんどのタスクを実行します。Web マネージャは、コンソールスイッチにネットワークアクセス可能な任意のコンピュータ上の Explorer® 6.0 および 7.0, そして Firefox® 2 および 3 で動作します。

管理者は、Web マネージャを使用して、ユーザーアカウントの作成、グループの承認、およびセキュリティとポートの設定を実行できます。承認ユーザーは、接続されたデバイスに Web マネージャを使用してアクセスし、それらのデバイスのトラブルシューティング、保守、電源の OFF/ON、接続デバイスの再起動、およびユーザーパスワードの変更を実行できます。Web マネージャの詳細は、第 3 章を参照してください。

IPv4 および IPv6 のサポート

コンソールスイッチは、デュアルスタックの IPv4 と IPv6 プロトコルに対応しています。管理者は Web マネージャまたは CLI を使用して、IPv4 のみ、または IPv4 と IPv6 の両方のアドレスのサポートを設定することができます。このコンソールスイッチに提供されている IPv6 サポートの一覧を次に示します。

- DHCP
- ダイヤルインセッション (PPP リンク)
- MergePoint Access 管理ソフトウェアの統合
- eth0 および eth1 の Ethernet インターフェイス
- ファイアウォール (IP テーブル)
- HTTP/HTTPS

- Linux カーネル
- リモート認証 : Radius, Tacacs+, LDAP 、および Kerberos サーバー
- SNMP
- SSH および Telnet アクセス
- Syslog サーバー

メモ : リモート認証の NIS、NFS および IPSec は、IPv6 ではサポートされていません。

柔軟なユーザーおよびグループ

コンソールスイッチ上または認証サーバー上の各ユーザーにアカウントを定義することができます。デフォルトのアカウントである admin ユーザーおよび root ユーザーは、どちらもその他のユーザーアカウントを追加および設定できます。管理者がカスタムユーザーグループに割り当てることができる承認に基づいて、ポートへのアクセスを必要に応じて制限することができます。詳細は、47 ページの「ユーザーアカウントとユーザーグループ」を参照してください。

セキュリティ

セキュリティプロファイルでは、コンソールスイッチで有効にするネットワークサービスを決定します。管理者は、有効なポートへのアクセスをすべてのユーザーに許可するか、グループ承認を設定してアクセスを制限することができます。また、有効にするサービス (FTP、ICMP、IPSec、Telnet)、および SSH と HTTP/HTTPS のアクセスを定義するセキュリティプロファイルを選択することもできます。管理者は、あらかじめ設定されたセキュリティプロファイルを選択することも、カスタムプロファイルを作成することもできます。詳細は 22 ページの「セキュリティ」を参照してください。

認証

認証は、ワンタイムパスワード (OTP) を利用してローカルで実行することも、リモートの Kerberos、LDAP、NIS、Radius、TACACS+ 認証サーバー、または MergePoint Access サーバーで実行することもできます。コンソールスイッチは、LDAP、Radius、および TACACS+ の各認証方法について、リモートのグループ承認もサポートしています。さらに、フォールバック機構も使用できます。

コンソールスイッチまたはポートに設定された認証方法は、Telnet、SSH、または Web マネージャを経由してログインを試行するすべてのユーザーの認証に使用されます。詳細は、44 ページの「認証」を参照してください。

NAT トラバーサル対応の IPSec ベースの VPN

選択したセキュリティプロファイルで IPSec が有効になっている場合、管理者は VPN 機能を使用してセキュアな接続を確立できます。オプションの NAT トラバーサル (デフォルト設定) が設定された IPSec 暗号化では、コンソールスイッチと、IPSec がインストールされたその他のコンピュータの間の専用通信用にセキュアなトンネルが作成されます。

ESP 認証プロトコル、AH 認証プロトコル、RSA 公開鍵、および共有シークレットがサポートされています。詳細は、30 ページの「IPSec(VPN)」を参照してください。

パケットフィルタリング

管理者は、ファイアウォールと同様にパケットをフィルターするようにコンソールスイッチを設定できます。パケットフィルタリングは、チェインで制御します。チェインとはユーザーが定義したルールを持つ名前付きプロファイルです。コンソールスイッチのフィルター一覧表には、変更することはできるが、削除できない組み込みのチェインが多数含まれています。

また、管理者は新しいチェインを作成したり、設定することができます

SNMP

選択したセキュリティプロファイル内で SNMP が有効の場合、管理者は SNMP 管理アプリケーションからの SNMP リクエストを受信したり、応答するためのコンソールスイッチ上の SNMP(Simple Network Management Protocol) エージェントを設定することができます。コンソールスイッチの SNMP エージェントは、SNMP v1/v2 と v3、MIB-II、および Enterprise MIB をサポートしています。詳細は、31 ページの「SNMP の設定」を参照してください。

メモ：Enterprise MIB および TRAP MIB のテキストファイルは、アプライアンスの /usr/local/mibs ディレクトリにあります。

データログ、通知、アラーム、およびバッファ

管理者は、電子メール、SMS、Syslog メッセージ、SNMP トラップ、または MergePoint Access ソフトウェア通知を用いて問題が管理者に警告されるように、データログ、通知、およびアラームを設定できます。また、管理者は、バッファデータをローカル、あるいは MergePoint Access 管理ソフトウェアを含むリモートに格納することもできます。コンソールスイッチおよび接続されたサーバーやデバイスに関するメッセージは、Syslog サーバーに送信することもできます。

電源管理

電源管理が承認されているユーザーは、コンソールスイッチから接続状態の PDU (Power Distribution Unit) に接続されているデバイスの電源をオンまたはオフにしたり、デバイスをリセットしたりできます。電源デバイスはいずれかのシリアルポートまたは AUX ポートに接続できます。詳細は、57 ページの「電源管理」を参照してください。

自動検出

メモ：管理者は、シリアルポートのホスト名を発見するための自動検出を有効にできます。自動検出用のデフォルトのプローブストリングおよび一致ストリングは、幅広く用意されています。管理者は、サイトに固有のプローブストリングおよび一致ストリングを設定できます。また、自動検出は、MergePoint Access ソフトウェア経由で設定することもできます。

構成例

次の図および表は、コンソールスイッチの一般的な構成を示しています。
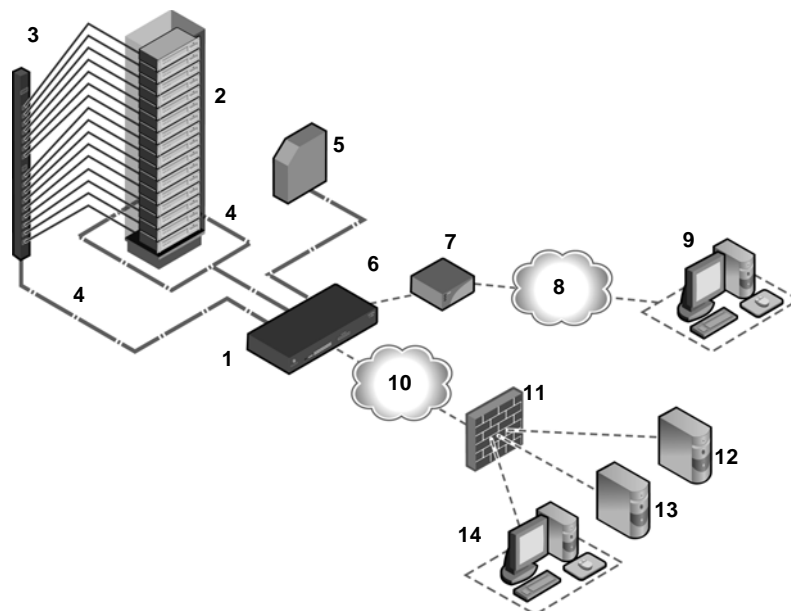
図 1.1: コンソールスイッチの一般的な構成

表 1.1: コンソールスイッチの一般的な構成の説明

番号	説明	番号	説明
1	SERVIS IP-Serial コンソールスイッチ	8	電話回線
2	ターゲットデバイス	9	リモートのダイヤルインクライアント
3	PDU (一台以上)	10	LAN (ローカルエリアネットワーク)
4	シリアルポート接続	11	LAN ファイアウォール
5	PC カード (モデム、Ethernet、または ストレージ)	12	リモートの認証サーバー
6	Either AUX またはいずれかのシリアルポート t	13	MergePoint Access サーバーあるいは FW クライアント
7	外部モデル	14	リモートまたはローカルの Windows/Linux コンピュータ

章
2

設置

はじめに

コンソールスイッチに同梱されているすべての物品、および適切な設置を行うために必要なその他の物品を所有していることを確かにするために次のリストを参照してください。

コンソールスイッチの梱包品

- 電源ケーブル
- Cat5 ストレートケーブル
- モデム接続用ケーブル
- D-sub25 メス⇔ RJ-45 変換アダプタ
- D-sub25 オス⇔ RJ-45 変換アダプタ
- D-sub9 メス⇔ RJ-45 変換アダプタ
- ループバックアダプタ
- フランジ
- フランジ用ネジ
- CD-ROM : 取扱説明書、統合管理ツール (FW クライアント) など
- 保証書
- 中国 RoHS 説明文
- クイックスタートガイド

その他の必要品

もし、スタンドアロン設定でコンソールスイッチを設定する場合、次の物品も必要です。

- 1 つ以上の Cat5 ストレートケーブル
- D-sub9 ⇔ RJ45 ストレートアダプタ
- PC で動作するターミナルエミュレーションプログラム

ラックへの搭載

コンソールスイッチは、ラックやキャビネットに搭載することも、机上やその他の平らな面に設置することもできます。ラックまたはキャビネットへの搭載用に、フランジ 2 個が付属しています。

コンソールスイッチをラックに取り付ける

1. SERVIS IP-Serial コンソールスイッチの前端部または後端部に、付属のネジを使用してフランジを取り付けます。
2. コンソールスイッチを安全な場所に取り付けます。

図 2.1: **前端部で搭載する場合の固定部品の取り付け**

ハードウェアの接続

コンソールスイッチのコネクタ

次の図は、コンソールスイッチの前面にあるコネクタを示しています。

図 2.2: **コンソールスイッチの前面** (32 **ポートモデル**)

表 2.1: **コンソールスイッチの前面のコネクタ**

番号	説明
1	USB コネクタ
2	LED。表 2.2 を参照してください。.
3	PC カードスロット

表 2.2: **コンソールスイッチの前面の** LED

ラベル	説明
PWR/CPU	青色 • 点滅 - ユニット起動中 • 点灯 - 動作中 • 消灯 - 電源オフ f
ETH 0/ETH 1	• 橙色 - 速度 10BaseT でリンク • 黄色 - 速度 100BaseT でリンク • 緑色 - 速度 1000BaseT でリンク • 消灯 - リンクなし、ケーブルが外れた状態、Ethernet 障害
AUX	デュアル LED • 黄色 - DTR/DCD のアクティビティ • 緑色 - TXD および RXD のアクティビティ • 消灯 - アクティビティなし
[各シリアルポートの LED(1 づつ)]	緑色 • 点滅 - 使用可能 (アクティビティあり) • 点灯 - 使用可能 • 消灯 - 使用不可

次の図は、コンソールスイッチの背面にあるコネクタを示しています。
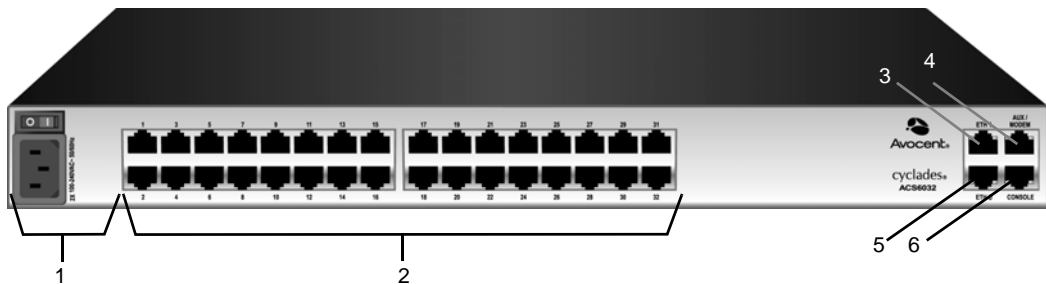
図 2.3: **コンソールスイッチの背面** (32 **ポートモデル**)

表 2.3: **コンソールスイッチの背面のコネクタ**

番号	説明
1	電源
2	シリアルポート (図は 32 個)。モデルによって 8 個、16 個、32 個、または 48 個のシリアルポートがあります。
3	ETH1 10/100M/1G Ethernet ポート。2 つめのネットワークに接続したり、フェイルオーバーに使用したりできます。
4	AUX ポート。このポートは､工場出荷時に RJ-45 コンソールスイッチのピン配列の RS-232 として定義されており、外部モデムまたは電源デバイスへの接続に使用できます。
5	リモート IP アクセス用 ETH0 10/100M/1G Ethernet ポート。.
6	CONSOLE ポート。ローカルで管理する場合、および端末または端末エミュレータのあるコンピュータを介して接続デバイスにアクセスする場合に使用できます。

デバイスコンソールまたはモデムとシリアルポートの接続

ターゲットデバイスコンソールまたはモデムをコンソールスイッチのシリアルポートに接続するには、CAT5 またはそれ以上のケーブルと、DB-9 または DB-25 コンソールアダプタを必要に応じて使用します。

コンソールスイッチでは、Cisco® シリアルポートピン配列の設定をサポートしており、その設定はデフォルトで無効になっています。ポートに Cisco ケーブルが接続されている場合、管理者はそのポートにおいて、Cisco ピン配列を有効にする必要があります。管理者は、物理的設定画面を開くために、「エキスパート」-「ポート」-「シリアルポート」- (CAS の設定、あるいは電源の設定) –「物理的」を選択し、そして「Cisco RJ45 ピン配列を有効にする」にチェックを入れます。

次の表は、シリアルポートピン配列の情報を示しています。

表 2.4: コンソールスイッチシリアルポートピン配列

ピン番号	信号名	入出力
1	RTS	OUT
2	DTR	OUT
3	TxD	OUT
4	GND	N/A
5	CTS	IN
6	RxD	IN
7	DCD/DSR	IN
8	未使用	N/A

表 2.5: Cisco シリアルポートピン配列

ピン番号	信号名	入出力
1	CTS	IN
2	DCD/DSR	IN
3	RxD	IN
4	GND	N/A
5	未使用	N/A
6	TxD	OUT
7	DTR	OUT
8	RTS	OUT

デバイス、モデムおよび PDU をシリアルポートに接続する

デバイスの接続に使用するクロスケーブルのピン配列のタイプが、ソフトウェア内でポートに設定されているタイプと同じであることを確認してください。

1. 接続するデバイスの電源スイッチがオフであることを確認します。
2. デバイスをコンソールスイッチに接続するには、CAT5 またはそれ以上のクロスケーブルを使用します。もし必要ならば、アダプタを使用します。
3. モデムを接続するには、モデムに適したコネクタまたはアダプタ (USB、DB-9、または DB-25) を用い、CAT5 またはそれ以上のストレートケーブルを使用します。

メモ：EMC の要件に準拠するために、すべてのポート接続にシールド付きケーブルを使用してください。

警告： コンソールスイッチをオンにしてから、接続されたデバイスの電源を入れてください。

電源デバイスのデイジーチェーン

次の図は、コンソールスイッチのシリアルポートにデイジーチェーン接続した 2 台の PDU を示しています。
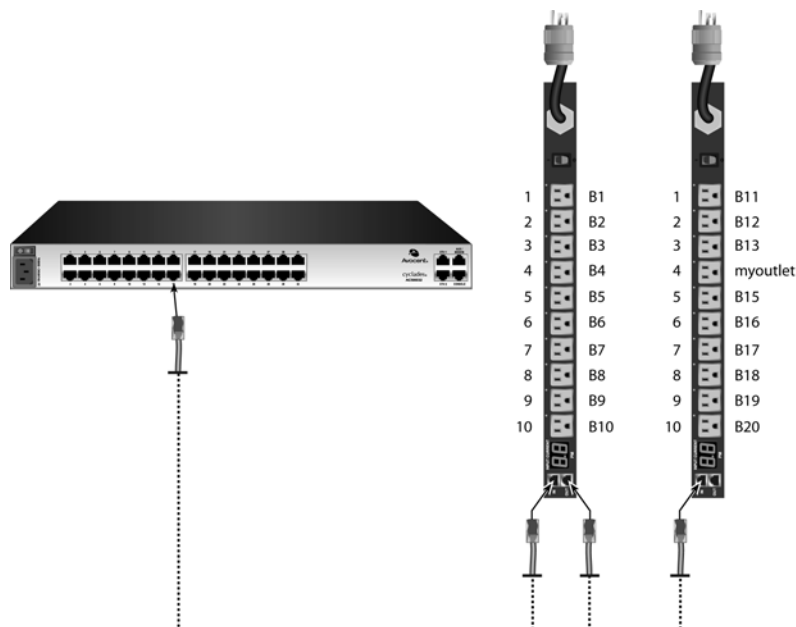
図 2.4: **デイジーチェーン接続した** PDU **の例**

PDU をコンソールスイッチにデイジーチェーン接続する

この手順は、コンソールスイッチの 1 つのシリアルポートに 1 台の PDU が接続されていることを前提としています。

1. 両端に RJ-45 コネクタの付いた UTP ケーブルの一方の端を、接続されている PDU の OUT ポートに差し込みます。
2. ケーブルのもう一方の両端を、2 台目の PDU の IN ポートに差し込みます。必要な数の PDU を接続するまで . 両方のステップを繰り返してください。

メモ：パフォーマンス上の理由から、1 つのシリアルポートに接続するコンセントは 128 個までにすることをお勧めします。

コンソールスイッチの電源投入

コンソールスイッチには、AC 電源機構が 1 つ付属しています。

警告： コンソールスイッチの電源をオフし、その後オンする場合は、その前に必ず Web マネージャ、CLI または MergePoint Access ソフトウェアの「エキスパート」–「システムツール」ノードからシャットダウンコマンドを実行してください。この操作によって、フラッシュ内のファイルシステムへのアクセス中にリセットが発生することはなくなり、フラッシュメモリの破損を防ぐことができます。

コンソールスイッチをオンにする

1. コンソールスイッチがオフであることを確認します。
2. 電源ケーブルを、コンソールスイッチと電源元に差し込みます。
3. コンソールスイッチの電源をオンにします。
4. 接続デバイスの電源スイッチをオンにします。

コンソールスイッチの設定

コンソールスイッチは、CONSOLE ポート経由あるいは SSH、Telnet セッションを用いてアクセスするコマンドラインインターフェイス (CLI) を通してアプライアンスの設定が出来ます。

メモ：MergePoint Access ソフトウェアを使用して設定する場合、MergePoint Access インストーラ / ユーザーガイドを参照してください。コンソールスイッチの Web マネージャを使用して設定する場合、17 ページの第 3 章を参照してください。Telnet あるいは SSH を使用して設定する場合、コンソールスイッチのコマンドリファレンスガイドを参照してください。

端末をコンソールスイッチの CONSOLE ポートに接続する

1. CAT 5 ストレートケーブルを端末、、または端末エミュレーションプログラム (ハイパーターミナル ® など) などが動作する PC とコンソールスイッチの背面パネル上の CONSOLE ポートに接続します。RJ-45 ポートをサポートしているモデルのため、RJ-45 ⇔ DB9 (メス) アダプタが添付されています .

   端末の設定は 9600bps, 8bit, 1 ストップビット , パリティなし、フロー制御なしです。

2. **admin** として、デフォルトのパスワード **admin** を使用してコンソールサーバーにログインします。CLI のプロンプトが表示されます。

   ```
   Welcome to SERVIS IP-Serial <FW-S1016SR-0C-2A-B6>.
   Type help for more information.
   --:- / cli->
   ```

3. コマンドプロンプトで **wiz** と入力して、現在の IP 設定を表示または変更します。

   ```
   --|- units cli-> wiz
   ```

4. Eth0 の IP 設定を設定します。現在の値をそのまま使用する場合は **Enter** を押し、オプションを表示する場合は **Tab + Tab** を押します。現在のパラメーター値を表示して編集する場合は **Esc + Tab** を押します。

```
current ipv4 address: 172.26.30.137
current ipv6 address:
eth0:
device_status = enabled
ipv4_method = dhcp
ipv4_address = 192.168.160.10
ipv4_mask = 255.255.255.0
ipv4_default_gateway =
ipv6_method = ipv6_address_unconfigured
ipv6_address =
ipv6_prefix_length =
ipv6_default_gateway =
mac address: 00:e0:86:0c:2a:b6

dns:
primary_dns = 172.26.29.4
secondary_dns =
domain = corp.avocent.com
hostname = FW-S1016SR-0C-2A-B6
```

5. **yes** と入力し新しい設定を確定して保存します。

   これらのパラメーターはすべて正しいですか ? (no, yes, quit) [no] :

メモ：DHCP はデフォルトの IP 設定です。ユーザーが Web マネージャにアクセスするには、固定の IP アドレスが使用可能である必要があります。

ネットワークへの接続

1. Ethernet ケーブルの一方の端をコンソールスイッチの背面パネル上の ETH 0 というラベルのポートに接続し、もう一方の端を Ethernet ハブまたはスイッチに接続します。
2. コンソールスイッチはデフォルトで DHCP が有効になっています。ユーザーは、DHCP から割り当てられた IP アドレス、管理者が割り当てた静的 IP アドレス、またはデフォルトの IP アドレス (192.168.160.10) のいずれかを使用して、Web マネージャにアクセスできます。

メモ：DHCP サーバーがネットワーク上にない場合、またはコンソールスイッチの IP アドレスを検出できなかった場合は、デフォルトの静的 IP/ サブネットマスクアドレスである 192.168.160.10/255.255.255.0 (eth0 の場合) および 192.168.161.10/255.255.255.0 (eth1 の場合) となります。操作 PC とコンソールスイッチの両方が同じ物理ネットワーク内になければなりません。ホストルート 192.168.160.10/32 を Ethernet インターフェイスに追加します。次の例は、Linux コンピュータ上のコンソールスイッチの eth0 にこのルートを追加します。

```
# route add - host 192.168.160.10 eth0
```

プラグ可能なデバイスの取り付けと設定

プラグ可能なデバイス (PC カードおよび USB デバイス) の挿入と設定を行う前に、プラグ可能なデバイスの検出を有効にする 必要があります。

メモ：内部データベース内の一覧にないプラグ可能なデバイスが検出された場合、「デバイス情報」列にはテキストが何も表示されないか、またはカードのタイプに基づいて異なるテキストが表示されます。たとえば、「Unknown device f024（rev 01）」などです。

プラグ可能なデバイスの検出を有効にする

1. Web マネージャで「プラグ可能なデバイス」を選択します。
2. 「プラグ可能なデバイスの検出を有効にする」をクリックします。

プラグ可能なデバイスを取り付ける

1. PC カードを使用可能なスロットに挿入する、または USB デバイスを接続します。
2. Web マネージャで「プラグ可能なデバイス」を選択します。「プラグ可能なデバイス」テーブルが表示され、検出されたプラグ可能なデバイスが表示されます。
3. デバイス名をクリックし、プラグ可能なデバイスのパラメーターを設定します。

メモ：ストレージデバイスは、自動的にマウントおよび設定されます。ワイヤレスデバイスの設定は、デバイスをいったん取り出してから再度挿入した後でのみ有効となります。

プラグ可能なデバイスを取り出す

メモ：プラグ可能なデバイスを取り出す場合は、必ず Web マネージャを使用してください。その他の方法を使用すると、カーネルパニックが発生する場合があります。

1. Web マネージャで「プラグ可能なデバイス」を選択します。
2. 取り出すプラグ可能なデバイスの名前の横にあるチェックボックスを選択して「イジェクト」をクリックし、プラグ可能なデバイスを取り出します。

プラグ可能なデバイスの名前を変更する（LAN デバイスで可能）

1. Web マネージャで「プラグ可能なデバイス」を選択します。
2. 名前を変更するプラグ可能なデバイスの名前の横にあるチェックボックスを選択して「名前の変更」をクリックします。
3. 新しい名前を入力し、「保存」をクリックします。

章

3

Webマネージャ経由でのコンソールスイッチへのアクセス

一度コンソールスイッチをネットワークに接続すれば、Web マネージャ経由でコンソールスイッチにアクセスすることができます。Web マネージャは、コマンドライン インターフェイスに代わって、グラフィカルユーザーインターフェイスによるコンソールスイッチへのダイレクトアクセスを提供します。

メモ：CLI あるいは MergePoint Access ソフトウェアでのコンソールスイッチへのアクセスの取扱説明書については、コンソールスイッチのコマンドリファレンスガイド あるいは、MergePoint Access インストーラ / ユーザーガイドを参照してください。

管理者向けの Web マネージャの概要

メモ：一般ユーザー向けの Web マネージャの概要については、62 ページの「一般ユーザー向けの Web マネージャの概要」を参照してください。

Web マネージャにログインする

1. Web ブラウザを開き、アドレスフィールドにコンソールスイッチの IP アドレスを入力します。
2. admin として、パスワード admin を使用する、あるいは root として、パスワード root を使用してログインします。

図 3.1 は、管理者向けの Web マネージャの一般的な画面を示しています。説明は、次の表 3.1 で示しています。
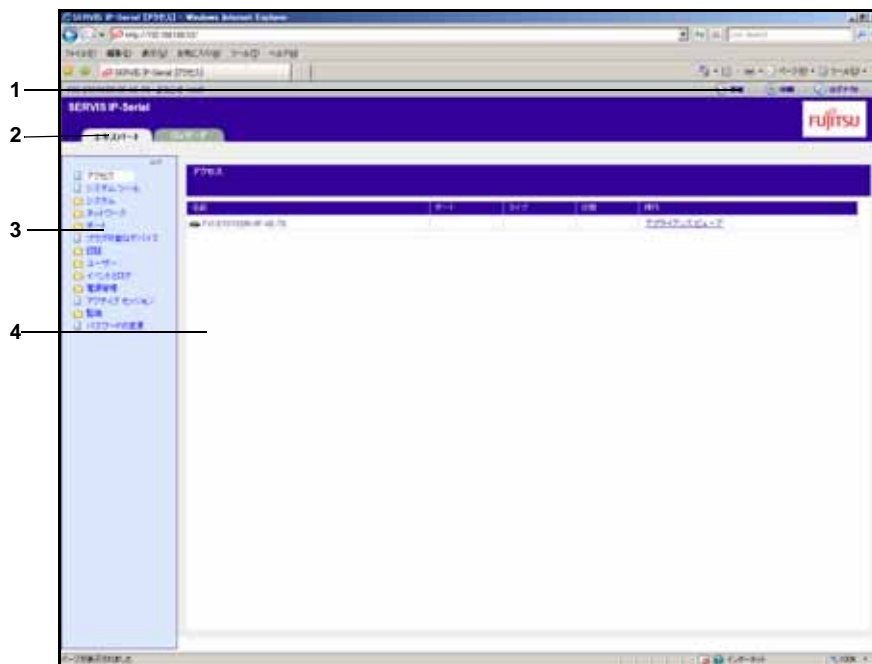
図 3.1: **管理者向けの** Web **マネージャの画面**

表 3.1: Web **マネージャ画面の各部**

番号	説明
1	最上部のオプションバー。左側にはアプライアンス名称、ログインしたユーザー名が表示されます。右側には「更新」、「印刷」、「ログアウト」ボタンが表示されます。.
2	タブバー。管理者は、「エキスパート」または「ウィザード」モードのどちらかを表示することができます。
3	サイドナビゲーションバー。設定、システム情報の表示、およびデバイスへのアクセスのためのメニューオプションがあります。オプションは、ユーザー権限によって異なります。
4	コンテンツ領域。内容はサイドナビゲーションバーで選択したオプションによって異なります。

ウィザードモード

ウィザードモードは、設定ステップを通して、管理者をガイドすることによって、設置や設定プロセスを容易にするようにデザインされています。管理者は、すべてのポートを CAS プロファイルに設定することができ、セキュリティプロファイル、ネットワーク、そしてユーザー設定をウィザードを利用して行うことができます。

デフォルトで、初めて Web マネージャでコンソールスイッチにアクセスする管理者には、ウィザードが表示されます。その後のログインは、エキスパートモードで開き、一度コンソールスイッチが設定されると、エキスパートモードがデフォルトとなります。管理者は、エキスパートモードとウィザードモードを管理者向け Web マネージャ画面上のタブバーをクリックすることによって、切替えることができます。

図 3.2 は、管理者がウィザードモードである場合の一般的な画面を示しています。
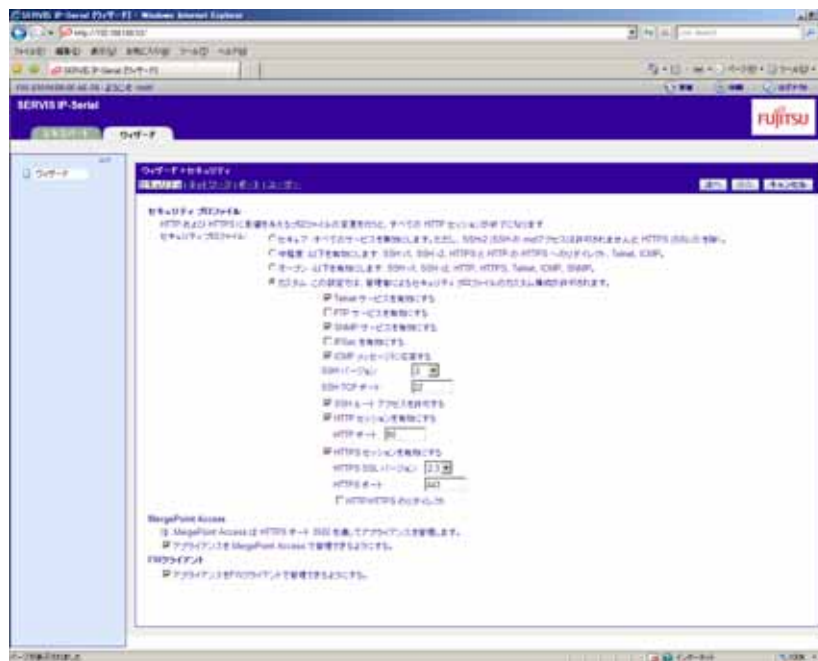
図 3.2: ウィザード画面

次の手順は、ウィザードからコンソールスイッチを設定する方法を説明しています。

セキュリティパラメーターを設定し、セキュリティプロファイルを選択する

1. コンテンツ領域の「セキュリティ」リンクを選択します。
2. 希望のセキュリティプロファイルを選択します。カスタムセキュリティプロファイルを使用する場合は、チェックボックスをクリックし、サイトのセキュリティポリシーに一致する SSH、HTTP および HTTPS オプションのようなサービスを設定するために必要に応じて値を入力します。
3. アプライアンス管理のために MergePoint Access ソフトウェアを使用しない場合、「アプライアンスを MergePoint Access で管理できるようにする。」チェックボックスのチェックを外します。

4. アプライアンス管理のために FW クライアントソフトウェアを使用しない場合、「アプライアンスを FW クライアントで管理できるようにする。」チェックボックスのチェックを外します。
5. ネットワークを設定するために、「次へ」をクリックします。あるいは、適切な画面を開くために 「ネットワーク」、「ポート」、あるいは「ユーザー」リンクをクリックします。

ネットワークをパラメーター設定する

1. コンテンツ領域の「セキュリティ」リンクを選択します。
2. ホスト名、プライマリ DNS、ドメインを適切なフィールドに入力します。
3. ETH0 インターフェイスの IPv4 あるいは ?IPv6 方式を選択します。静的を使用する場合は、アドレス、マスクおよびゲートウェイを適切なフィールドに入力します。
4. ポートを設定するために、「次へ」をクリックします。あるいは、適切な画面を開くために 「セキュリティ」、「ポート」、あるいは「ユーザー」リンクをクリックします。

ポートの設定

1. コンテンツ領域の「ユーザー」リンクを選択します。
2. 「すべてのポートを有効にする」チェックボックスをチェックし、Cisco ケーブルを接続している場合は、「Cisco RJ45 ピン配列を有効にする」チェックボックスにチェックをします。
3. 適切なドロップダウンメニューを使用し、速度、パリティ、データビット、ストップビット、フロー制御、プロトコル、認証タイプ、およびデータバッファの状態 を選択します。
4. データバッファタイプを選択します。NFS を使用する場合、NFS サーバーおよび NFS パス 情報を適切なフィールドに入力します。
5. ユーザーを設定するために、「次へ」をクリックします。あるいは、適切な画面を開くために「ネットワーク」、「セキュリティ」、あるいは「ユーザー」リンクをクリックします。

ユーザーを設定し、デフォルトのユーザーパスワードを変更する

警告：セキュリティ上の理由から、root ユーザーおよび admin ユーザーの両方のデフォルトパスワードをすぐに変更することをお勧めします。

1. コンテンツ領域の「ユーザー」リンクを選択します。
2. ユーザー名（admin あるいは root）をクリックし、パスワード、パスワードの確認フィールドに新しいパスワードを入力します。

   あるいは、ユーザーを追加するために、「追加」をクリックします。新しいユーザー名、パスワードを適切なフィールドに入力します。

3. （省略可能）ユーザーにパスワードの変更を強制するには、「ユーザーは次回のログインでパスワードを変更する必要があります。」のチェックボックスを選択します。
4. ユーザーを 1 つまたは複数のグループに割り当てます。
5. （省略可能）アカウントの有効期限およびパスワードの期限を設定します。
6. 「次へ」をクリックする。
7. ステップ 3 ～ 7 を必要に応じて繰り返し、新しいユーザーアカウントを設定し、デフォルトのグループに割り当てます。

メモ：デフォルトでは、設定されたすべてのユーザーが、すべての有効なポートにアクセスすることができます。サイトのセキュリティポリシーによって、ポートへのユーザーのアクセスを制限する必要がある場合は、追加の設定が必要です。

8. 「保存」をクリックし、その後「完了」をクリックします。

エキスパートモード

次のタブは、管理者がエキスパートモードである場合の Web マネージャのサイドナビゲーションバーにおいて、利用可能なものです。

アクセス

コンソールスイッチに接続されたすべてのデバイスを表示するために「アクセス」をクリックします。

Web マネージャを使用してデバイスを表示またはデバイスに接続する

1. サイドナビゲーションバーで「アクセス」を選択します。コンテンツ領域に、コンソールスイッチの名前と、ユーザーがアクセスを承認されている取り付け済みおよび設定済みのすべてのデバイスの名称あるいはエイリアスの一覧が表示されます。
2. 「操作」列から「シリアルビューア」を選択します。Java アプレットビューアが表示されます。
3. プロンプトが表示されたらログインします。

次の表は Java アプレットにおいて、利用できるボタンについて説明しています。.

表 3.2: コンソールスイッチに接続するための Java アプレットのボタン

ボタン	目的
SendBreak	端末へ break を送信する。
Disconnect	Java アプレットを切断する。
	左側のアイコンを選択するとサーバーあるいはデバイスに再接続します。また、右側のアイコンを選択すると Java アプレットからのセッションを終了し、切断します。

システムツール

システムツールをクリックすると、コンソールスイッチの再起動、シャットダウン、コンソールスイッチのファームウェアのアップグレード、コンソールスイッチ構成の保存、復元、あるいは、コンソールスイッチの SSH セッションを開くためにクリックすることができるアイコンが表示されます。

システム

システムツールをクリックすると、コンソールスイッチの再起動、シャットダウン、コンソールスイッチのファームウェアのアップグレード、コンソールスイッチ構成の保存、復元、あるいは、コンソールスイッチの SSH セッションを開くためにクリックすることができるアイコンが表示されます。

セキュリティ

セキュリティプロファイルでは、コンソールスイッチで有効にするネットワークサービスを決定します。

コンソールスイッチの管理者は、サイトのセキュリティポリシーに沿ったセキュリティパラメーターを設定する必要があります。次のようなセキュリティ機能を Web マネージャ、CLI、または MergePoint Access ソフトウェアで設定できます。

- セッションアイドルタイムアウトの設定
- RPC の有効化または無効化
- 有効にした
- セキュリティプロファイルを選択して次の内容を定義
  - 有効にするサービス (FTP、ICMP、IPSec 、Telnet)
  - SSH および HTTP/HTTPS アクセス

管理者は、あらかじめ設定されたセキュリティプロファイルを選択することも、カスタムプロファイルを作成することもできます。

各セキュリティプロファイルに対して有効または無効になっている、すべてのサービスと SSH および HTTP/HTTPS 設定オプションは、「ウィザード」-「セキュリティ」、および 「システム」-「セキュリティ」-「セキュリティプロファイル」ページで確認できます。

セキュリティプロファイルを設定する

1. 「システム」-「セキュリティ」-「セキュリティプロファイル」を選択します。
2. コンソールスイッチが開いているセッションをタイムアウトする前に、「アイドルタイムアウト」フィールドに秒数を入力します。

メモ：この値は、HTTP、HTTPS、SSH、Telnet あるいは CONSOLE ポート経由のアプライアンスへのいかなるユーザーセッションにも適用されます。新しいアイドルタイムアウトは、新規セッションにのみ適用されます。

3. 「有効なサービス」セクションの下にある「RCP」チェックボックスを有効または無効にします。
4. 「シリアルデバイス」という見出しの下にある、「ポートへのアクセスは、ユーザーグループに割り当てられた承認に基づいて制御されます」チェックボックスを有効または無効にします。
5. 「セキュリティプロファイル」という見出しの下にある、「カスタム」、「中程度」、「オープン」、または「セキュア」を選択します。
6. アプライアンスを管理するために FW クライアントソフトウェアを使用しない場合、「アプライアンスを FW クライアントで管理できるようにする。」チェックボックスのチェックを外します。
7. 「保存」をクリックする。

また、MergePoint Access ソフトウェアのセキュリティ設定を設定することもできます。コンソールスイッチが MergePoint Access ソフトウェアによって管理されている場合、MergePoint Access サーバーがコンソールスイッチに証明書を与えます。標準状態において、MergePoint Access ソフトウェアは、証明書のクリアや必要に応じて新規証明書に置き換えるという管理を行います。MergePoint Access ソフトウェアとの通信が失われた場合、MergePoint Access サーバーは、証明書のクリアができなくなり、コンソールスイッチを使用することができません。Trust All モードでコンソールスイッチを設定するために「MergePoint Access 証明書を消去する」ボタンをクリックします。

MergePoint Access ソフトウェアセキュリティの設定を実行する

1. 「システム」-「セキュリティ」-「MergePoint Access」を選択します。
2. 「アプライアンスを MergePoint Access で管理できるようにする。」チェックボックスをクリックし、「保存」をクリックします。

日付と時刻

コンソールスイッチでは、日付と時刻の設定用に 2 つのオプションが用意されています。コンソールスイッチは、ネットワークタイムプロトコル (NTP) サーバーから日付と時刻を取得することができます。また、日付と時刻を手動で設定して、コンソールスイッチの内部クロックにこの日付と時刻の情報を使用させることもできます。

メモ :「日付と時刻」画面の「現在の時刻」は、画面が開いたときの時刻のみを示します。継続的にリアルタイムに更新されることはありません。

NTP で日付と時刻を設定する

1. 「システム」-「日付と時刻」をクリックします。
2. 「ネットワークタイムプロトコル (NTP) を有効にする」を選択します。
3. 選択する NTP サーバーサイトを入力し、「保存」をクリックします。

主導で日付と時刻を設定する

1. 「システム」-「日付と時刻」をクリックします。
2. 「手動で設定」を選択します。
3. プルダウンメニューから必要な日付と時刻を選択し、「保存」をクリックします。

既定のタイムゾーンを使用してタイムゾーンを設定する

1. 「システム」-「日付と時刻」-「タイムゾーン」をクリックします。
2. 「既定」を選択します。
3. プルダウンメニューから必要なタイムゾーンを選択し、「保存」をクリックします。

カスタムタイムゾーン設定を定義する

1. 「システム」-「日付と時刻」-「タイムゾーン」をクリックします。
2. 「タイムゾーンを定義する」を選択します。
3. 選択する「タイムゾーン名」と「標準時刻の頭字語」を入力します。
4. GMT 補正を入力します。
5. 必要に応じて、「デーライトセービングタイムを有効にする」を選択します。
6. デーライトセービングタイム設定に必要な値を選択または入力し、「保存」をクリックします。

言語

「システム」-「言語」をクリックし、プルダウンメニューからコンソールスイッチの言語を選択します。「保存」をクリックします。

起動構成

起動構成では、コンソールスイッチでオペレーティングシステムのロード元とする場所を定義します。コンソールスイッチは、内部ファームウェアまたはネットワークから起動できます。デフォルトでは、コンソールスイッチはフラッシュメモリから起動します。「システム」-「起動構成」をクリックすると、「起動構成」画面が表示されます。

ネットワークから起動する必要がある場合は、次の前提条件が満たされていることを確認します。

- TFTP または BootP サーバーがネットワーク上で使用可能
- アップグレード済みのコンソールスイッチブートイメージファイルを TFTP または BootP サーバーで使用可能
- コンソールスイッチが固定 IP アドレスで設定済み
- TFTP または BootP サーバーの起動ファイル名と IP アドレスが既知

起動構成を設定する

1. 「システム」-「起動構成」をクリックします。「起動構成」画面が表示されます。

2. 「起動モード」の下で、「フラッシュから」を選択し、「イメージ 1」または「イメージ 2」を選択します。

   または

   「ネットワークから」を選択し、次の情報を入力します。

   - 「アプライアンス IP アドレス」: 固定 IP アドレス、または DHCP がコンソールスイッチに割り当てた IP アドレスを入力します。
   - 「TFTP サーバー IP」: TFTP 起動サーバーの IP アドレスを入力します。
   - 「ファイル名」: 起動ファームウェアのファイル名を入力します。

3. プルダウンメニューを使用し、ウォッチドッグタイマーを有効にするか無効にするかを選択します。ウォッチドッグタイマーが有効な場合、ソフトウェアがクラッシュしたときにコンソールスイッチが再起動します。
4. プルダウンメニューを使用し、「Ethernet 0 モード」および「Ethernet 1 モード」の速度をそれぞれ「100BT (全)」、「100BT (半)」、「10BT (全)」、「10BT (半)」、または「自動」から 1 つ選択します。
5. プルダウンメニューを使用し、「コンソール速度」を選択し、「保存」をクリックします。

メモ : Ethernet モードは、保存後に反映されます。他の設定は、再起動後に適用されます。

情報

「システム」-「情報」をクリックするとコンソールスイッチの ID、バージョン、および CPU 情報が表示されます。

使用状況

「システム」-「使用状況」をクリックするとメモリーおよびフラッシュの使用が表示されます。

ネットワーク

「ネットワーク」をクリックするとホスト名、DNS、IPv6、結合、IPv4 および IPv6 静的経路、ホスト、ファイアウォール、IPSec(VPN)、および SNMP を表示して設定ができます。

設定

ネットワーク設定を変更するために、「ネットワーク」-「設定」をクリックします。

デバイス

管理者は、ネットワークインターフェイスに割り当てる IP アドレスを選択、有効化、および設定し、MAC アドレスを参照できます。標準的な 2 つの Ethernet インターフェイス

に加え、取り付ける可能性のあるすべての Ethernet PC カードに対応するネットワークインターフェイスが用意されています。

ネットワークデバイスを設定する

1. 「ネットワーク」-「デバイス」を選択します。「デバイス」画面に、ネットワークインターフェイスの一覧と、それらが有効か無効かを示す状態が表示されます。
2. 設定するネットワークデバイスの名前をクリックします。
3. ドロップダウンメニューから「有効」または「無効」の状態を選択します。
4. IPv4 方式のオプションを次の中から選択します。
   - DHCP サーバーで IPv4 IP アドレスを設定するには、「DHCP」を選択します。
   - IPv4 IP アドレスとサブネットマスクを手動で入力するには、「静的」を選択します。
   - IPv4 を無効にするには、「IPv4 アドレスが未構成」を選択します。
5. IPv6 方式のオプションを次の中から選択します。
   - リンクがローカル IP アドレスに限られる場合は、「状態に依存しない」を選択します。
   - DHCP サーバーで IPv6 IP アドレスを設定するには、「DHCPv6」を選択します。
   - IPv6 IP アドレスと接頭辞長を手動で入力するには、「静的」を選択します。
   - IPv6 を無効にするには、「IPv6 アドレスが未構成」を選択します。
6. 内蔵インターフェイス（ETH0 あるいは ETH1）の Ethernet モードを選択します。

メモ：このオプションに続いてデバイスの MAC アドレスが表示されます。

メモ：次のステップは、ワイヤレス Ethernet PC カードでのみアクティブです。

7. 次のワイヤレス LAN 情報を入力します。
   a. ワイヤレスアクセスポイントのユニークな ID を入力するには、「マイプライベートネット」を選択します。
   b. アクセスポイントの通信チャネルを入力するには、「チャネル」を選択します。
   c. 送信中のデータ暗号化を有効にするには、「暗号化」を選択します。
   d. 受信する暗号化データをデコードするためのキーおよびパスワードを入力し、「保存」をクリックします。

IPv4 静的経路および IPv6 静的経路

静的経路を追加する

1. 「ネットワーク」-「IPv4 静的経路」または「IPv6 静的経路」を選択します。既存の静的経路があれば表示され、その「送信先 IP/ マスク」、「ゲートウェイ」、「インターフェイス」、および「メトリック」の値も表示されます。
2. 「追加」をクリックします。

3. 「デフォルト」を選択し、デフォルトの経路を設定します。

   または

   「ホスト IP またはネットワーク」を選択し、「送信先 IP/ マスク」のカスタム設定を入力します。

   必要な送信先 IP/ マスクビットを、< 送信先 IP>/< サブネットマスク >/<CIDR> という構文で「送信先 IP/ マスクビット」フィールドに入力します。
4. ゲートウェイの IP アドレスを「ゲートウェイ」フィールドに入力します。
5. 送信先までのホップ数を「メトリック」フィールドに入力し、「保存」をクリックします。

ホスト

管理者は、ローカルネットワークのホスト名、IP アドレス、およびホストエイリアスの一覧を設定できます。

ホストを追加する

1. 「ネットワーク」-「ホスト」を選択します。
2. 「追加」をクリックし、新しいホストを追加します。
3. 追加するホストの IP アドレス、ホスト名、およびエイリアスを入力し、「保存」をクリックします。

ホストを編集する

1. 「ネットワーク」-「ホスト」を選択します。
2. 編集するホスト名の IP アドレスをクリックします。
3. 新しいホスト名とエイリアスを適切に入力し、「保存」をクリックします。

ファイアウォール

管理者は、コンソールスイッチをファイアウォールとして動作するように設定できます。デフォルトでは、3 つの組み込みチェインで、INPUT、FORWARD、および OUTPUT パケットのすべてが受け入れられます。「追加」、「削除」、または「ポリシーの変更」ボタンを選択することで、ユーザーチェインの追加、ユーザーが追加したチェインの削除、および組み込みチェインのポリシーの変更が可能です。デフォルトチェインのポリシーについては、「ポリシーの変更」での変更を受け入れるか破棄できますが、削除することはできません。「チェイン名」をクリックすると、チェインのルールを設定できます。

ファイアウォールは、「ネットワーク」-「ファイアウォール」をクリックすると設定できます。「IPv4 フィルター一覧表」または「IPv6 フィルター一覧表」メニューオプションでも、同じ設定画面を個別に表示できます。

デフォルトチェインについてはポリシーのみ編集できます。デフォルトチェインのポリシーのオプションは ACCEPT と DROP です。

チェインが追加されると、そのチェイン用の名前付きエントリーのみが作成されます。チェインの追加後に、1 つ以上のルールを設定する必要があります。

ファイアウォールの設定

「ターゲット」プルダウンメニューから、各ルールに「ACCEPT」、「DROP」、「RETURN」、「LOG」、または「REJECT」のいずれかのアクションを選択する必要があります。選択したアクションは、ルールに指定されたすべての条件を満たす IP パケットに対して実行されます。

「ターゲット」プルダウンメニューから「LOG」を選択した場合、管理者は「ログレベル」および「ログの識別番号」を設定し、「ログオプション」セクションで「TCP シーケンス」、「TCP オプション」、および「IP オプション」をログに記録するかどうかを設定できます。

「ターゲット」プルダウンメニューから「REJECT」を選択した場合、管理者は「拒否の理由」のプルダウンメニューでオプションを選択できます。パケットは破棄され、選択したタイプの応答パケットが送信されます。

プロトコルのオプション

「プロトコル」プルダウンメニューの各オプションに対して、異なるフィールドがアクティブになります。

「プロトコル」メニューから「数字」を選択した場合は、テキストフィールドに「プロトコル番号」を入力します。

「プロトコル」メニューから「TCP」を選択した場合は、「TCP オプション」セクションがアクティブになるので、ここにソースポートおよび送信先ポートと、TCP フラグを入力します。

「プロトコル」メニューから「UDP」を選択した場合は、「UDP」セクションがアクティブになるので、ソースポートおよび送信先ポートを入力します。

表 3.3: 「ファイアウォールの設定」-「TCP」および「UDP」オプションフィールド

フィールドまたはメニューオプション	定義
「ソースポート」または「送信先ポート」	単一の IP アドレスの範囲
「TCP フラグ」	(TCP のみ) SYN (同期)、ACK (確認応答)、FIN (完了)、RST (リセット)、URG (緊急)、および PSH (プッシュ)。各フラグのプルダウンメニューの条件は、「緊急」、「セット」または「セットの解除」。

「プロトコル」メニューから「ICMP」を選択した場合、「ICMP タイプ」プルダウンメニューがアクティブになります。

入力または出力インターフェイスのフィールドに管理者が eth0 または eth1 の Ethernet インターフェイスを入力し、「フラグメント」プルダウンメニューから「2 番目以降のパケット」、「すべてのパケットとフラグメント」、または「分割されていないパケットおよび最初のパケット」のオプションを選択した場合、指定したインターフェイスとの間で送受信されるパケットが選択した「フラグメント」メニューオプションの条件に一致すると、そのパケットに対してターゲットのアクションが実行されます。

チェインの追加する

1. 「ネットワーク」-「ファイアウォール」を選択します。
2. 必要に応じて、「IPv4 フィルター一覧表」または「IPv6 フィルター一覧表」のいずれかを選択します。
3. 「追加」をクリックします。
4. 追加するチェインの名前を入力します。
5. 「保存」をクリックします。

メモ：チェイン名には空白文字を使用できません。

6. 1 つ以上のルールを追加し、チェインの設定を完了します。

デフォルトチェインのポリシーを変更する

メモ：ユーザーが定義したチェインは編集できません。ユーザーが追加したチェインの名前を変更するには、削除してから新しく作成します。

1. 「ネットワーク」-「ファイアウォール」を選択します。
2. 必要に応じて、「IPv4 フィルター一覧表」または「IPv6 フィルター一覧表」のいずれかを選択します。
3. 変更するチェイン（「FORWARD」、「INPUT」、または「OUTPUT」）の名前の横にあるチェックボックスを選択します。
4. 「ポリシーの変更」をクリックし、プルダウンメニューから「承認」または「中断」を選択します。
5. 「保存」をクリックします。

ルールを追加する

1. 「ネットワーク」-「ファイアウォール」を選択します。
2. 必要に応じて、「IPv4 フィルター一覧表」または「IPv6 フィルター一覧表」のいずれかを選択します。
3. チェインの一覧で、ルールを追加するチェインの名前をクリックします。
4. 「追加」をクリックして、必要に応じてルールを設定し、「保存」をクリックします。

ルールを編集する

1. 「ネットワーク」-「ファイアウォール」を選択します。

2. 必要に応じて、「IPv4 フィルター一覧表」または「IPv6 フィルター一覧表」のいずれかを選択します。
3. チェインの一覧で、ルールを編集するチェインの名前をクリックします。
4. 編集する「ルール番号」をクリックします。
5. 必要に応じてルールを変更し、「保存」をクリックします。

IPSec(VPN)

仮想プライベートネットワーク (VPN) では、ゲートウェイを利用してコンソールスイッチとゲートウェイの間にセキュアな接続を作成することにより、コンソールスイッチとリモートネットワークとの間でセキュアな通信を実現できます。IPSec は、セキュアトンネルを構築するために使用するプロトコルです。IPSec では、プロトコルスタックの IP レベルで暗号化サービスや認証サービスが提供されます。

メモ：IPSec(VPN) は IPv6 ではサポートされていません。

「ネットワーク」-「IPSec(VPN)」を選択すると、「IPSec(VPN)」画面が表示されます。

「追加」ボタンを使用して VPN 接続を追加するか、既存の接続名をクリックしてリスト内の接続を編集します。「削除」ボタンをクリックすると、既存の接続が削除されます。NAT の設定を変更する必要がある場合は、「NAT の構成」ボタンをクリックします。

「追加」ボタンをクリックすると、「IPSec(VPN) - 追加」画面が表示されます。

メモ：IPSec(VPN) を動作させるには、カスタムセキュリティプロファイルで IPSec を有効にする必要があります。

リモートのゲートウェイをリモートまたは右ホスト、コンソールスイッチをローカルまたは左ホストと呼びます。右ホストと左ホストを直接接続しない場合は、次のホップの IP アドレスも指定する必要があります。

リモートつまり右ホストの次のホップは、IPSec を利用しているゲートウェイまたはリモートホストが左ホストへパケットを送信するときに送信先とするルーターの IP アドレスです。左ホストの次のホップは、コンソールスイッチが右ホストへパケットを送信するときに送信先とするルーターの IP アドレスです。

IPSec ネゴシエーションを行うローカル (左) ホストおよびリモート (右) ホストの両方の「ID」フィールドに、完全修飾ドメイン名が表示されるようにしてください。

「IPSec(VPN) - 追加」画面のフィールドおよびオプションを次の表にまとめます。これらの情報は、ローカルとリモートの両側で正確に一致させる必要があります。

表 3.4: IPSec (VPN) の設定に関するフィールドおよびメニューオプション

フィールド名	定義
「接続名」	接続の識別に使用する、任意の記述的な名前。

表 3.4: IPSec (VPN) の設定に関するフィールドおよびメニューオプション

フィールド名	定義
「認証プロトコル」	使用する認証プロトコルで、ESP(カプセル化セキュリティペイロード) または AH(認証ヘッダー)。
起動設定	ホストに設定する起動操作で「開始」、「経路」、「追加」または「無視」。
「認証方法」	使用する認証方法で、「RSA キー」または「シークレット」。
「リモート (右) 側」 および 「ローカル (左) 側」	リモート側およびローカル側の 4 つのフィールドに、それぞれ必要なアドレスまたはテキストを入力します。 「ID」**:** ローカルシステムおよびリモートシステムで IPSec ネゴシエーションや認証に使用するホスト名。@ のあとに完全修飾ドメイン名を指定できます。たとえば、**hostname@xyz.com** のように入力します。 「IP アドレス」**:** ホストの IP アドレス。 「次のホップ」**:** コンソールスイッチ (左側) またはリモートホスト (右側) で相手側のホストにパケットを送信する際に経由するルーター。 「サブネット」**:** ホストが属するサブネットワークのマスク。 CIDR 表記を使用します。IP 番号に続いて、スラッシュと、2 進数表記にしたネットマスクの「1」ビットの数を指定します。たとえば 192.168.0.0/24 は、最初の 24 ビットがネットワークアドレスとして使用される IP アドレスを表します。これは、255.255.255.0 と同等です。
「RSA キー」(RSA キーが選択された場合)	IPSec (VPN) 認証では、コンソールスイッチの公開鍵を生成し、リモートゲートウェイで使用されている鍵を調べる必要があります。別のソースから RSA キーをコピーしてペーストすることもできます。
「事前共有シークレット」(「シークレット」が認識された場合)	右側および左側のユーザー間で事前に共有するパスワード。

SNMP の設定

管理者は SNMP を設定できます。SNMP は、コンソールスイッチが SNMP 管理アプリケーションに管理される場合に必要になります。

SNMP を設定する

1. 「ネットワーク」-「SNMP」をクリックします。
2. 「システム」ボタンをクリックします。
    a. SysContact 情報、つまりコンソールスイッチの管理者の電子メールアドレスを **servis-center@fcl.fujitsu.com** のように入力します。
    b. SysLocation 情報、つまりコンソールスイッチの物理的な場所を入力し、「保存」をクリックして SNMP 画面に戻ります。
3. 「追加」をクリックし、新規コミュニティあるいは、v3 ユーザーを追加します。
4. 「名前」フィールドに、SNMP v1/v2 のコミュニティ名、または SNMP v3 のユーザー名を入力し、「OID」を入力します。

5. プルダウンメニューから必要なパーミッションを選択します。「読み取り / 書き込み」または「読み取り専用」を選択します。
6. 必要な SNMP のバージョンが v1 または v2 の場合は、「バージョン v1/v2」ボタンをクリックしてソース (有効な入力はサブネットアドレスです。) を入力します。

   または

   必要な SNMP のバージョンが v1 または v2 で IPv6 ネットワークを使用する場合は、「IPv6 ネットワーク用バージョン v1/v2」ボタンをクリックしてソース（ソースに入力できるのはサブネットアドレスです。）を入力します。

   または

   必要な SNMP のバージョンが v3 の場合は、「バージョン v3」ボタンをクリックして「認証タイプ」に MD5 または SHA を選択します。「認証パスフレーズまたはパスワード」を入力し、「DES のプライバシーパスフレーズ」を入力して「最小のセキュリティレベル」(NoAuthNoPriv、AuthNoPriv、AuthPriv) を選択します。
7. 「保存」をクリックします。

ポート

管理者は、シリアルポートおよび補助ポートを有効にして設定できます。また、サイドナビゲーションバーのポートタブから CAS プロファイルおよびダイヤルインプロファイルを設定することができます。補助ポートの画面では、補助ポートを有効にし、接続するデバイスのタイプに基づいて設定できます。

シリアルポート

シリアルポート一覧表では、接続するデバイスのタイプに基づいて接続プロファイル（CAS、ダイヤルイン、電源）を指定することができ、ポートをクローン化する、工場設定に戻す、ポートを有効 / 無効にすることができます。

1 つ以上のシリアルポートに対して有効化または無効化を行う

1. 「ポート」-「シリアルポート」を選択します。
2. 有効化または無効化する各ポートのチェックボックスをクリックします。
3. 「有効」または「無効」ボタンをクリックします。

1 つ以上のシリアルポートの CAS プロファイルを設定あるいは編集する

1. 「ポート」-「シリアルポート」を選択します。
2. 設定する各ポートのチェックボックスをクリックします。
3. 「CAS の設定」ボタンをクリックします。
   a. 選択したポートに Cisco 製ケーブルを接続した場合に、デフォルトのピン配列を変更するには、「Cisco RJ45 ピン配列を有効にする」チェックボックスを選択します。

b. プルダウンメニューからポートの有効もしくは無効、速度、パリティ、データビット、ストップビット、フロー制御を設定します。
4. 「次へ」をクリックする、あるいは、「CAS」リンクをクリックします。
   a. 1 つのポートのみが選択されている場合、ポート名を入力します。あるいは、2 つ以上のポートが選択されている場合、ポート名プリフィックスを入力します。ポート名は、< ポート名プリフィックス >-p-< ポート番号 > となります。
   b. 自動検出を有効にするためにチェックボックスにチェックを入れます。

メモ : 速度自動検出は、「CAS プロファイル」-「自動検出設定」画面で追加設定が必要です。

---

   c. 適切なプルダウンメニューからプロトコルおよび認証タイプを設定します。
   d. 「テキストセッションのホットキー」および「電源セッションのホットキー」を適切なフィールドに入力します。
   e. 「TCP ポートエイリアス」を適切なフィールドに入力します。
   f. 「IPv4 エイリアス」、「IPv6 エイリアス」、「IPv4 エイリアスインターフェイス」、および「IPv6 エイリアスインターフェイス」を適切なフィールドに入力します。
   g. 「DCD がオンの場合のみセッションを許可する」および「自動応答を有効にする」には、適切なチェックボックスを選択します。
   h. プルダウンメニューから DTR モードを選択し、DTR オフ間隔を入力します。
   i. プルダウンメニューから「ラインフィード抑制」および「CR 抑制後は Null 値」の有効あるいは無効を選択します。
   j. 「送信間隔」、「ブレークシーケンス」、および「ブレーク間隔」を適切なフィールドに入力します。
   k. プルダウンメニューから「マルチセッションのログイン / ログアウトの通知」、および「情報メッセージの通知」を選択します。
5. 「次へ」をクリックする、あるいは、「データバッファ」リンクをクリックし、プルダウンメニューからデータバッファ設定の有効、あるいは 無効を設定します。
6. 「次へ」をクリックする、あるいは、「アラート」リンクをクリックします。
   a. アラートの検出を有効にするために「アラートを有効にする」をクリックします。
   b. アラートストリングを追加するために、「追加」ボタンをクリックします。「アラートストリング」フィールドに文字列を入力し、「次へ」をクリックして、アラート画面に戻ります。
   c. 既存のアラートの横にあるチェックボックスにチェックを入れ、「削除」をクリックするとそのストリングは削除されます。
   d. 「任意を削除」をクリックすると選択されているストリング、あるいは選択されていないストリングのすべてのストリングを削除します。

メモ :「任意を削除」をクリックするとすべてのアラートストリングが削除されます。すべてのアラートストリングを選択し、「削除」をクリックすることとは機能が異なります。すべてのアラートストリングを選択し、「削除」をクリックする場合は、テーブルに表示されていないアラートストリングは削除されません。

7. 「次へ」をクリックする、あるいは、「電源」リンクをクリックします。
   a. 新規のコンセントを追加するために「追加」をクリックします。
   b. 既存の結合されているコンセントの横にあるチェックボックスにチェックを入れ、「削除」をクリックするとそのコンセントは削除されます。

メモ : 1 つのシリアルポートが選択されている場合にのみ電源は有効となります。

8. 「保存」をクリックします。

表 3.5: CAS **プロファイルパラメーター**

パラメーター	**説明**
物理的	
Cisco RJ-45 ピン配列を有効にする	シリアルポートのピン配列を定義します。デフォルト設定 : 無効
状態	シリアルポートの状態を有効あるいは無効のいずれかとして定義します。デフォルト : 無効
速度	速度を 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 あるいは 115200 のいずれかに定義する。デフォルト : 9600
パリティ	パリティを偶数、奇数あるいはなしのいずれかに定義します。デフォルト : なし
データビット	データビットを 5, 6, 7 あるいは 8 のいずれかに定義します。デフォルト : 8
ストップビット	ストップビットを 1 あるいは 2 のいずれかに定義します。デフォルト : 1
フローコントロール	フロー制御をなし、ハードウェア、ソフトウェア、RxON ソフトウェアあるいは TxON ソフトウェアのいずれかに定義します。デフォルト : なし
CAS	
ポート名	名称をシリアルポートと (エイリアスとして) 関連付けます。デフォルト : < アプライアンスの MAC アドレス >-p-< ポート番号 >
自動検出を有効にする	ターゲットの名称を検出し、このシリアルポートと関連付けます。失敗した場合、ポート名が使用されます。デフォルト : 無効
速度自動検出を有効にする	シリアルポートの速度の検出を試行します。この機能は、「CAS プロファイル」-「自動検出」-「設定」ページで追加設定が必要です。デフォルト : 無効

表 3.5: CAS プロファイルパラメーター (続き)

パラメーター	説明
プロトコル	シリアルポートあるいはターゲットデバイスにアクセスするために使用するプロトコルです。 • SSH - SSH セッション . • Telnet - Telnet セッション . • SSH/Telnet - SSH および Telnet セッションを許可します。 デフォルト：SSH/Telnet
認証タイプ	ターゲットセッション中にユーザーを認証するために使用する認証タイプです。デフォルト：ローカル
テキストセッションのホットキー	ターゲットセッションを一時停止し、CLI プロンプトに移行するためのホットキーです。デフォルト：^Z (Ctrl-Z)
電源セッションのホットキー	ターゲットセッションを一時停止し、ターゲットに結合されているコンセントを制御するための電源管理メニュー表示するためのホットキーです。デフォルト：^P (Ctrl-P)
TCP ポートエイリアス	Telnet セッション : シリアルポートに直接接続するための TCP ポートです。 SSH セッション：ttySxx と同様のポートエイリアスです。 デフォルト：70XX、XX はシリアルポート番号です。
ポート IPv4/IPv6	シリアルポートに直接接続するための IPv4/IPv6 アドレスです。 デフォルト：未設定（空欄）
ポート IPv4/IPv6 エイリアスインターフェイス	IPv4/IPv6 エイリアスと関連付けるインターフェイス (ETH0/ETH1) です。デフォルト：ETH0
DCD がオンの場合のみセッションを許可する	DCD がオフの場合、アプライアンスはシリアルポートへのアクセスを拒否します。デフォルト：無効 (DCD がオフの場合でもアクセスが許可される)
自動応答を有効にする	入力データが自動応答で設定されたある入力ストリングに一致した場合、出力ストリングがシリアルポートに送信されます。 デフォルト：無効
DTR モード	DTR モードは次のように設定されます。 ・ 常時オン ・ 通常 -DTR 状態は、CAS セッションの存在によって決まります。 ・ オフ間隔 -CAS セッションが閉じられた場合、DTR はこの間隔の間、ダウン状態となる。 デフォルト：通常
DTR オフ間隔	DTR モードのオフ間隔で使用されるミリ秒単位の秒間隔です。 デフォルト：100
ラインフィード抑制	CR 文字の後に、LF 文字の抑制を有効にします。 デフォルト：無効

表 3.5: CAS **プロファイルパラメーター** (**続き**)

パラメーター	**説明**
CR 抑制後は Null 値	CR 文字の後に、NULL 文字の抑制を有効にします。 デフォルト：無効
送信間隔	リモートクライアントへデータ送信するためのミリ秒単位のポートの待ち間隔です。デフォルト：20
ブレークシーケンス	シリアルポートへ break 信号を送信するために使用されるシーケンスです。デフォルト：~break
ブレーク間隔	ミリ秒単位の break 信号の間隔です。デフォルト：500
マルチセッションのログイン / ログアウトの通知	新規ユーザーがログインあるいはユーザーがログアウトした場合、マルチセッションユーザーへの通知を有効にします。デフォルト：無効
情報メッセージの通知	ターゲットセッションが開始された場合、情報メッセージが表示されます。
データバッファ	
状態	データバッファを有効あるいは無効にします。デフォルト：無効
タイプ	データバッファのタイプを表示します。 • ローカル - ローカルファイルシステムにデータバッファリングファイルを保存します。 • NFS -NFS サーバー上にデータバッファリングファイルを保存します。 • Syslog - syslog サーバーにデータを送信します。 • MergePoint Access- MergePoint Access ソフトウェアにデータを送信します。 デフォルト：ローカル
タイムスタンプ	有効の場合、ローカルあるいは NFS サーバーのデータバッファ行にタイムスタンプを付加します。デフォルト：無効
ログイン / ログアウトメッセージ	データバッファにおいて、ログインおよびログアウトの特別通知を含みます。デフォルト：無効
シリアルセッションログ	• 有効 – 常にデータを保存します。 • 無効 – CAS プロファイルが開始されていない場合、データを保存します。 デフォルト：有効
アラート	
状態	入力データがあるアラートストリングに一致した場合、特別なイベント通知が発生します。デフォルト：無効
アラートストリングス	イベント通知を発生させるために使用されるストリングです。デフォルト：空

モデムが接続されたシリアルポートにダイヤルインプロファイルを設定する

1. 「ポート」-「シリアルポート」を選択します。
2. モデムが接続されたシリアルポートのチェックボックスをクリックします。
3. 「ダイヤルインの設定」ボタンをクリックし、ダイヤルインの設定を行うためにプルダウンメニューを使用します。
4. PPP パラメーター（アドレス、認証など）を設定し、「保存」をクリックします。

表 3.6: ダイヤルインパラメーター

パラメーター	説明
状態	ポートを有効あるいは無効にします。デフォルト：無効
速度	mgetty でシリアルデバイスを設定するために使用される速度です。 デフォルト：38400bps
チャットの初期化	モデムの初期化のためのチャットです。 デフォルト： `"" ¥d¥d¥d+++¥d¥d¥d¥ATZ OK`
PPP アドレス	PPPリンクのためのローカルおよびリモートのIPアドレスを設定します。「リモートピアからの構成を受け入れる」を選択している場合、リモートピアはネゴシエーションの間、（ローカルおよびリモートの）両方の IP アドレスに送信されます。デフォルト：アドレスなし
ローカル IPv4/IPv6 アドレス	PPP 接続のローカルの IPv4/IPv6 アドレスを設定します。
リモート IPv4/IPv6 アドレス	PPP 接続のリモートの IPv4/IPv6 アドレスを設定します。
PPP 認証プロトコル	ラジオボタンで選択します：なし、PAP、CHAP、あるいは EAP • なし - 認証なし • PAP - PAP プロトコルを使用し、認証タイプは、PPP 認証タイプ（「認証」-「ユニット認証」ページで設定）で設定します。 • CHAP - CHAP プロトコルを使用します。CHAP シークレットの設定は、/etc/ppp/chap-secrets ファイルを編集している間に実施されます。 • EAP - EAP プロトコルを使用します。利用可能な認証は：CHAP、SRP-SHA1 および TLS です。CHAP のシークレットの設定は、/etc/ppp/chap-secrets ファイルを編集している間に実施されます。SRP-SHA1 のシークレットの設定は、/etc/ppp/srp-secrets ファイルを編集している間に実施されます。 • デフォルト：なし

表 3.6: ダイヤルインパラメーター (続き)

パラメーター	説明
CHAP	CHAP-間隔、CHAP-チャレンジ-最大回数とCHAP-再起動を設定します。 デフォルト設定 : CHAP- 間隔 = 0 CHAP- チャレンジ - 最大回数 = 10 CHAP- 再起動 = 3 PPP アイドルタイムアウト
PPP アイドルタイムアウト	PPP タイムアウトするまでのアイドル秒数です。デフォルト : 0（タイムアウトなし）.

PDU が接続された 1 つ以上のシリアルポートを設定あるいは編集する

1. 「ポート」-「シリアルポート」を選択します。
2. PDU が接続された 1 つ以上のシリアルポートのチェックボックスをクリックします。
3. 「電源の設定」ボタンをクリックし、物理的設定を行うためにプルダウンメニューを使用します。
4. 「次へ」をクリックする、あるいは「電源」リンクをクリックします。
   a. PDU タイプを選択するためにプルダウンメニューを使用します。
   b. 速度自動検出を有効にするためにチェックボックスにチェックを入れます。
   c. ポーリングレートを設定します。
   d. 電源のオフ / オンの間隔を入力し、その後 Syslog、ブザー、SW 過電流保護を有効にする、あるいは無効にするためにプルダウンメニューを使用します。
5. 「保存」をクリックします。

表 3.7: 電源パラメーター

パラメーター	説明
物理的	
Cisco RJ-45 ピン配列を有効にする	シリアルポートのピン配列を定義します。デフォルト設定 : 無効
状態	シリアルポートの状態を有効あるいは無効のいずれかとして定義します。デフォルト : 無効
速度	速度を 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 あるいは 230400 と定義します。デフォルト : 9600
パリティ	パリティを偶数、奇数あるいは なし のいずれかに定義します。デフォルト : なし

表 3.7: 電源パラメーター (続き)

パラメーター	説明
データビット	データビットを 5，6，7 あるいは 8 のいずれかに定義します。デフォルト : 8
ストップビット	ストップビットを 1 あるいは 2 のいずれかに定義します。デフォルト : **1**
フロー制御	フロー制御を なし、ハードウェア、ソフトウェア、RxON ソフトウェア あるいは TxON ソフトウェアのいずれかに定義します。デフォルト : なし
電源	
PDU タイプ	シリアルポートに接続されている PDU のタイプを定義します。
速度自動検出を有効にする	有効の場合、ポートの速度を検出します。デフォルト : 無効
ポーリングレート	PDU からの情報を更新する秒間隔です。デフォルト : 20
電源のオフ / オン間隔	電源オフ / オンコマンドのための オフ動作とオン動作の間の秒間隔です。デフォルト : 15
Syslog	有効の場合、PDU はアプライアンスに syslog メッセージを送信します。デフォルト : 有効
ブザー	PDU のブザーを有効あるいは無効にします。デフォルト : 有効
SW 過電流保護	有効の場合、ソフトウェアの過電流保護がオンになります。デフォルト : 無効

他のポートの設定を複製あるいはクローンする

1. 「ポート」-「シリアルポート」を選択します。
2. クローン（複製）するシリアルポートのチェックボックスをクリックします。
3. 「クローン」ボタンをクリックします。
4. 「構成を次に対して複製する」フィールドに設定を行うシリアルポートを入力し、「保存」をクリックします。

メモ : 選択されたポートが CAS プロファイルとして設定されている場合、次のパラメーターは複製されません : ポート名、TCP ポートエイリアス、ポート IPv4 エイリアス、ポート IPv6 エイリアス および 電源（結合されているコンセント)。

1 つ以上のシリアルポートを工場設定に戻す

1. 1 つ以上のシリアルポートを工場設定に戻す
2. 工場設定に戻す 1 つ以上のシリアルポートのチェックボックスをクリックし、「工場設定に戻す」ボタンをクリックします。

メモ：シリアルポートは工場設定において、CAS プロファイルに設定され、無効となります。

補助ポート

補助ポートの画面では、補助ポートを有効にし、接続するデバイスのタイプに基づいて設定できます。

PDU が接続された補助ポートを設定あるいは編集する

1. 「ポート」-「補助ポート」を選択します。
2. 「電源の設定」ボタンをクリックし、物理的設定を行うためにプルダウンメニューを使用します。
3. 「次へ」をクリックする、あるいは「電源」リンクをクリックします。
   a. PDU タイプを選択するために、プルダウンメニューを使用します。
   b. 速度自動検出を有効にするためにチェックボックスにチェックを入れます。
   c. ポーリングレートを設定します。
   d. 電源のオフ / オンの間隔を入力し、その後 Syslog、ブザー、SW 過電流保護を有効にする、あるいは無効にするためにプルダウンメニューを使用します。
4. 「保存」をクリックします。

モデムが接続された補助ポートを設定あるいは編集する

1. 「ポート」-「補助ポート」を選択します。
2. 「ダイヤルインの設定」ボタンをクリックし、ダイヤルインの設定を行うためにプルダウンメニューを使用します。
3. PPP パラメーター ー (アドレス、認証など) を設定します。
4. 「保存」をクリックします。

CAS プロファイル

管理者は、自動検出機能 および 自動応答機能の設定を行うことができます。

自動検出

自動検出機能は、シリアルポートに接続されたサーバーのターゲット名称を検出します。この名称は、シリアルポートのエイリアスとして使用されます。

特定のシリアルデバイスのために自動検出がアクティブである場合、ターゲット接続 (DCD ON イベント) において、アプライアンスは、プローブストリングを送信し、正規表現を用いたターゲットデバイスの応答を分析し始めます。ユーザー定義のプローブストリングおよび一致ストリング は、もちろん 定義済みのプローブストリングおよび一致ストリングもあります。

それぞれのプローブストリングを送信するために、一致ストリングによって定義されたすべての正規表現がテストされます。最後のサイクルが終わると、シーケンスは再ス

タートします。この手順は、特定の期間（自動検出タイムアウトパラメーターで設定された）あるいは、ターゲットが正常に検出されるまで実行されます。自動検出に失敗した場合、ターゲット名称は、対応する唯一のデフォルトのターゲット名称にリセットされます。

プローブストリングは、サーバーの応答を促す ("¥n" のような単一の改行文字) ために使用されます。

一致ストリングは、正規表現で、"%H" は検出するターゲット名称の代替となります。例えば、" ¥¥(.*¥¥)(%H)¥¥(.*¥¥)" あるいは、"xxx%Hyyy" です。

一つ目のストリングは、ターゲット名称を抽出します。例えば、

```
nanana(myTarget): à results: myTarget
jhdsgjhas(tg2)kjafja à results: tg2
```

しかし、一致するのは、

`hsagdfjhagfxxxTARGETyyyyyy à resulting: TARGET` です。

自動検出で使用されるプローブストリングまたは一致ストリングを設定する

自動検出で使用されるデフォルト設定や、プローブストリングまたは一致ストリングを変更するには、この手順を実行します。

1. 「ポート」-「CAS プロファイル」-「自動検出」を選択します。サイドナビゲーションバーに「設定」、「プローブストリング」および「一致ストリング」オプションが表示されます。
2. デフォルトの自動検出タイムアウトまたはプローブタイムアウトを変更するには、次の手順を実行します。
   a. 「設定」を選択します。
   b. 「自動検出タイムアウト」および 「プローブタイムアウト」フィールドに新しい値を入力します。
   c. 「自動検出エラー時のデフォルト速度」ドロップダウンメニューおよび「検査速度の一覧」で速度を選択します。
   d. 「保存」をクリックします。
3. 新しいプローブストリングまたは一致ストリングを追加するか、既存のストリングを削除するには、次の手順を実行します。
   a. 「プローブストリング」または「一致ストリング」を選択します。
   b. ストリングを追加するには、「追加」をクリックして「新規プローブストリング」または「新規一致ストリング」フィールドに新しいストリングを入力し、「保存」をクリックします。
   c. ストリングを削除するには、そのストリングのチェックボックスを選択して「削除」をクリックします。
4. 「保存」をクリックします。

自動応答で使用される入力ストリングまたは出力ストリングを設定する

1. 「ポート」-「CAS プロファイル」-「自動応答」を選択します。
2. 自動応答の入力ストリングおよび出力ストリングを追加するには、「追加」をクリックします。「入力ストリング」または「出力ストリング」フィールドに新しいストリングを入力し、「保存」をクリックします。

   または

   自動応答の入力ストリングおよび出力ストリングを削除するには、対応するチェックボックスを選択して、「削除」をクリックし、その後「保存」をクリックします。

ダイヤルインのプロファイル

管理者は、OTP ログイン、PPP 接続、PPP/PAP 認証、コールバック、PPP 接続用の OTP ユーザーなどの、セキュアダイヤルイン設定を行うことができます。

メモ：プラグ可能なデバイスをダイヤルアウト用に使用している場合、ダイヤルインは無効にします。

ダイヤルインプロファイルが設定されたポートにセキュアダイヤルイン設定を行う

1. 「ポート」-「ダイヤルインプロファイル」-「設定」を選択します。
2. コンソールスイッチに対するモデム経由のログインを有効にし、ログインを許可する条件を選択するには、次の手順を実行します。
   a. コールバック接続のみを許可するには、「コールバック」を選択します。
   b. あらゆる接続を許可するには、「有効にする」を選択します。
3. OTP 認証を有効にするには、「OTP ログイン認証」メニューから「有効にする」を選択します。
4. OTP 認証を有効にするには、「OTP ログイン認証」メニューから「有効にする」を選択します。
   a. PPP コールバック接続のみを許可するには、「コールバック」を選択します。
   b. あらゆる接続を許可するには、「有効にする」を選択します。
5. ポートに PAP 認証プロトコルが設定されている場合は、「PPP/PAP 認証」メニューからこの認証タイプを選択します。
6. 「保存」をクリックします。

ダイヤルインプロファイルが設定されたポートに、ユーザーへのコールバックと電話番号を設定する

1. 「ポート」-「ダイヤルインプロファイル」-「セキュアダイヤルイン」-「ユーザーへのコールバック」を選択します。
2. 「追加」をクリックします。

3. 適切なフィールドに、コールバックの実行に使用する 名前、および電話番号を入力し、「保存」をクリックします。

ダイヤルインプロファイルが設定されたポートに PPP OTP ユーザーを設定する

1. 「ポート」-「ダイヤルインプロファイル」-「セキュアダイヤルイン」-「PPP OTP ユーザー」を選択します。
2. 「追加」をクリックします。
3. 適切なフィールドに ユーザー名、およびパスフレーズを入力し、「保存」をクリックします。

メモ : この PPP OPT ユーザーが PPP 接続を確立するのは、正常に認証されたあとです。

ダイヤルインプロファイルが設定されたポートに、PPP 認証として EAP-TLS を設定する

1. 「ポート」-「シリアルポート」を選択します。

   または

   「ポート」-「補助ポート」を選択します。

2. モデムが接続されたポートの横にあるチェックボックスにチェックを入れ、「ダイヤルインの設定」をクリックします。
3. PPP アドレス設定を行います。例えば、ローカル IPv4 アドレスとして 10.0.0.1 をリモート IPv4 アドレスとして 10.0.0.2 を使用して、ローカル構成の PPP アドレスを設定します。
4. PPP 認証で、「アプライアンス別」の横にあるボタンを選択し、その後、プロトコルで「EAP」の横にあるボタンを選択します。「保存」をクリックします。
5. 「ポート」-「ダイヤルインプロファイル」-「設定」を選択します。
6. ドロップダウンメニューを使用して PPP 接続を「有効にする」にし、「保存」をクリックします。
7. 証明書およびキーを /etc/ppp/cert にコピーします。それらは、server.crs (コンソールスイッチの証明書) 、ca.crt (認証局の証明書)、server.key (スイッチの非対称暗号鍵) と名付けられます。

プラグ可能なデバイス

プラグ可能なデバイスを管理する

1. プラグ可能なデバイスの検出が有効の場合、「プラグ可能なデバイス」を選択します。

   または

プラグ可能なデバイスの検出が無効の場合、「プラグ可能なデバイスの検出を有効にする」をクリックします。

2. 設定対象とするプラグ可能なデバイスの横にあるチェックボックスを選択するか、プラグ可能なデバイスの一覧の上部にあるチェックボックスですべてのデバイスを選択します。
3. 「すべてインストール」、「イジェクト」、または「名前の変更」をクリックします。
4. 検出を無効にするには、「プラグ可能なデバイスの検出を無効にする」をクリックします。

プラグ可能なデバイスの情報を表示して変更する

1. 「プラグ可能なデバイス」を選択し、プラグ可能なデバイスの名前を選択します。
2. プラグ可能なデバイスのタイプが「ネットワーク」の場合、「ネットワーク / デバイス」セクションが表示されてネットワークパラメーターの設定が可能になります。

   または

   プラグ可能なデバイスのタイプがモデム（V.92 またはワイヤレス）の場合、「ダイヤルイン / デバイス」セクションが表示され、ダイヤルインパラメーターの設定が可能になります。

認証

認証は、OTP を利用してローカルで実行することも、リモートの Kerberos、LDAP、NIS、Radius、または TACACS+ 認証サーバー上で実行することもできます。コンソールスイッチが MergePoint Access サーバーによって管理されている場合、MergePoint Access 認証もサポートします。コンソールスイッチは、LDAP、Radius、および TACACS+ の各認証方法について、リモートのグループ承認もサポートしています。

次のようなフォールバック機構を利用できます。

最初にローカル認証を試行し、ローカル認証が失敗した場合にリモート認証を試行 (ローカル → 認証失敗 → リモート)

または

最初にリモート認証を試行し、そのあとローカル認証を試行 (リモート → 認証失敗 → ローカル)

または

リモート認証サーバーに障害が発生している場合にのみ、ローカル認証を試行 (リモート → 認証不可 → ローカル)。

管理者は、CLI ユーティリティや Web マネージャを使用して認証を設定できます。コンソールスイッチおよびシリアルポートのデフォルトの認証方法はローカルです。コンソールスイッチまたはポートに設定された認証方法は、Telnet、SSH、または Web マネージャ を経由してログインを試行するすべてのユーザーの認証に使用されます。

アプライアンスの認証

コンソールスイッチでは、コンソールスイッチおよびポートが、グループ別または個別に認証されます。

メモ：グループ承認を使用する場合は、コンソールスイッチおよびすべてのシリアルポートの両方に同じ認証を使用するか、シングルサインオン認証を使用してグループ承認を容易にすることをお勧めします。

シングルサインオン認証が無効になっていると、コンソールスイッチでは個々のポートの設定が使用されます。ユーザーは個々のポートにアクセスするたびに、パスワードを使用する必要があります。シングルサインオン認証が有効になっていると、プルダウンメニューで選択した認証サーバーがすべてのポートに対して使用されるため、以後のポートへのアクセスについては認証が不要になります。

メモ：プルダウンメニューから「未設定」を選択すると、ポートで個別の認証サーバーを使用し続けることができます。この場合、最初にいずれかのポートにアクセスするときにパスワードが必要になります。以後のアクセスでは、シングルサインオン認証が有効になっていれば、ポートのパスワード認証は不要になります。

コンソールスイッチに認証を設定する

1. 「認証」-「アプライアンス認証」をクリックします。
2. 「認証タイプ」ドロップダウンメニューで必要な認証サーバーを選択します。
3. 「シングルサインオンを有効にする」を選択してシングルサインオン認証を有効にし、「認証タイプ」ドロップダウンメニューで必要な認証サーバーを選択します。
4. 「保存」をクリックします。

認証サーバー

認証サーバーを使用する場合は、事前にその IP アドレスを設定し、ほとんどの場合はその他のパラメーターも設定する必要があります。RADIUS、TACACS+、LDAP(S)|AD、Kerberos、NIS および MergePoint Acess の各認証サーバーには設定が必要です。

RADIUS 認証サーバーを設定する

1. 「認証」-「認証サーバー」-「RADIUS」を選択します。
2. 「第一認証サーバー」および「第一アカウンティングサーバー」の IP アドレスを入力します。
3. 必要に応じて、「第二認証サーバー」および「第二アカウンティングサーバー」の IP アドレスを入力します。
4. 「シークレット」フィールドに、シークレットワードつまりパスフレーズを入力し、「シークレットの確認」フィールドにもパスフレーズを入力します。このパスフレーズは、第一および第二認証サーバーと、アカウンティングサーバーに適用されます。
5. 「タイムアウト」フィールドに、サーバーがタイムアウトするまでの秒数を入力します。
6. 「再試行」フィールドに、再試行の回数を入力します。

7. 「[サービス タイプを有効にする] の属性を使用して、承認グループを指定します」チェックボックスを選択した場合は、「サービスタイプログイン」、「サービスタイプフレーム」、「サービスタイプコールバックログイン」、「サービスタイプコールバックフレーム」、「サービスタイプアウトバウンド」、「サービスタイプ管理」のそれぞれについて承認グループ名を入力します。
8. 「保存」をクリックします。

TACACS+ 認証サーバーを設定する

1. 「認証」-「認証サーバー」-「TACACS+」を選択します。
2. 「第一認証サーバー」および「第一アカウンティングサーバー」の IP アドレスを入力します。
3. 必要に応じて、「第二認証サーバー」および「第二アカウンティングサーバー」の IP アドレスを入力します。
4. 「サービス」ドロップダウンメニューから必要なサービス（「PPP」、「Raccess」または「シェル」）を選択します。
5. 「シークレット」フィールドに、シークレットワードつまりパスフレーズを入力し、「シークレットの確認」フィールドにもパスフレーズを入力します。このパスフレーズは、第一および第二認証サーバーと、アカウンティングサーバーに適用されます。
6. 「タイムアウト」フィールドに、サーバーがタイムアウトするまでの秒数を入力します。
7. 「再試行」フィールドに、再試行の回数を入力します。
8. 「shell の [ユーザーレベルを有効にする] の属性と raccess を使用して、承認グループを指定します」チェックボックスを選択した場合は、最大 15 のユーザーレベルの承認グループ名を入力します。
9. 「保存」をクリックします。

LDAP(S)|AD 認証サーバーを設定する

1. 「認証」-「認証サーバー」-「LDAP(S)|AD」を選択します。
2. サーバーの IP アドレスを入力します。
3. 「ベース」を入力します。
4. 「セキュア」ドロップダウンメニューから「オフ」、「オン」、または「Start_TLS」を選択します。
5. 「データベースユーザー名」を入力します。
6. 「データベースパスワード」を入力し、「パスワードの確認」フィールドにもそのデータベースパスワードを入力します。
7. 必要な「ログイン属性」を入力します。
8. 「保存」をクリックします。

Kerberos 認証サーバーを設定する

1. 「認証」-「認証サーバー」-「Kerberos」を選択します。
2. サーバーの IP アドレス (レルム) を入力します。
3. 「レルムドメイン名」を corp.com のように入力します。
4. 「ドメイン名」を **corp.com** のように入力します。
5. 「保存」をクリックします。

NIS 認証サーバーを設定する

1. 「認証」-「認証サーバー」-「NIS」を選択します。
2. サーバーの「NIS ドメイン名」を corp.xxx.com のように入力します。
3. 「NIS サーバーまたは “**broadcast**”」を入力します。デフォルトは broadcast です。
4. 「保存」をクリックします。

MergePoint Access 認証サーバーを設定する

1. 「認証」-「認証サーバー」-「MergePoint Access」を選択します。
2. 関連のフィールドに MergePoint Access サーバーの「IP アドレス 1 ～ 4」を入力します。
3. 「保存」をクリックします。

ユーザーアカウントとユーザーグループ

管理者がカスタムユーザーグループに割り当てることができる承認に基づいて、ポートへのアクセスを必要に応じて制限することができます。グループに、デバイスへの接続中に電源を管理する権限を与えることもできます。コンソールスイッチには、admin と root の 2 つのデフォルトユーザーと、admin、appliance-admin、shell-login-profile および user の 4 つの既定ユーザーグループがあります。

コンソールスイッチ上または認証サーバー上の各ユーザーにユーザーアカウントを定義する必要があります。admin ユーザーおよび root ユーザーはデフォルトでアカウントを持ち、どちらの管理者もその他のユーザーのアカウントを追加および設定できます。各ローカルユーザーアカウントは、1 つ以上のユーザーグループに割り当てられます。

注意 : コンソールスイッチを動作させる前に、root および admin のデフォルトのパスワードを変更してください。

ローカルアカウント

admin と root は、同等のユーザーです。管理者はいつでも一般ユーザーにパーミッションを付与できます。コンソールスイッチには、次の 3 タイプのユーザーアカウントがあります。

- admin: 初期ネットワーク設定を実行します。admin のデフォルト設定のパスワードは **admin** です。admin ユーザーは admin グループのメンバーであり、admin ユーザーは、

コンソールスイッチおよびポートを設定できます。また、admin はユーザーやグループ承認を設定することもできます。

- root: admin ユーザーと同等のパーミッションを持ちます。root のデフォルト設定のパスワードは **root** です。コンソールスイッチでは、root ユーザーは admin グループおよび shell-login-profile グループのメンバーです。root ユーザーが CONSOLE ポート、SSH あるいは Telnet 経由でログインする場合、セッションは、シェルに直接移行するようにログインプロファイルによって事前に定義されています。
- 管理者が追加した一般ユーザー : 割り当てられたグループに基づいて、Web マネージャの機能に制限付きでアクセスできます。ユーザーは自身のパスワードを変更できます。デフォルトでは、どのユーザーもすべての有効なポートにアクセスできます。

新しいユーザーを追加する

1. 「ユーザー」-「ローカルアカウント」-「ユーザー名」をクリックします。「ユーザー名」画面にすべてのユーザーが一覧表示されます。
2. 「追加」をクリックします。「ユーザー名」画面が表示されます。
3. 新しいユーザー名を入力し、パスワードを入力し、その後パスワードの確認を入力します。
4. 「ユーザーは次回のログインでパスワードを変更する必要があります。」チェックボックスを選択するか、選択を解除します。
5. 利用できるユーザーグループにユーザーを追加するには、左のボックスでユーザーグループ名を選択して「追加」をクリックします。デフォルトのグループは user です。右のボックスでユーザーグループを選択して「削除」をクリックすると、ユーザーグループを削除できます。
6. 「パスワードの期限切れ」に必要なパラメーターを入力します。
   - 「最小日数」: パスワードの変更間隔として許可する最小日数を入力します。これより短期間のうちにパスワードを変更しようとすると拒否されます。指定しない場合のデフォルトは 0 になっています。
   - 「最大日数」: パスワードの有効期間の最大日数を入力します。この期間を過ぎると、パスワードの変更が強制されます。指定しない場合のデフォルトは 99999 になっています。
   - 「警告日数」: 期限切れの前にユーザーに警告を発行するまでの日数を入力します。0 を入力すると、期限切れの当日に警告が発行されます。マイナスの値を入力するか、値を入力しない場合、警告は発行されません。
7. 必要な「アカウントの有効期限」の日付を **YYYY-MM-DD** の形式で入力します。
8. 「保存」をクリックします。

パスワードのルールを設定する

1. 「ユーザー」-「ローカルアカウント」-「パスワードのルール」をクリックします。

2. パスワードを強制する場合は、「パスワードがセキュリティ要件のとおりに構成されているか確認してください」が選択されていることを確認します。パスワードは強制することをお勧めします。
3. 「パスワードの強制」を有効にする場合は、パスワードの設定要件に必要な値を入力します。
4. 「デフォルトの有効期限」に必要な値を入力します。
5. 「保存」をクリックします。

ユーザーグループ

ユーザーグループには、デフォルトの、または管理者が割り当てた、アクセス権および承認が与えられています。管理者は、appliance-admin または user グループに属するユーザーのパーミッションやアクセス権を変更するか、カスタムのパーミッションやアクセス権を設定したグループを追加作成できます。管理者は、どのグループのユーザーについても、パーミッションやアクセス権の追加、削除、または変更をいつでも行うことができます。

コンソールスイッチでポートへのユーザーアクセスに制限を設定する場合、管理者は、ポートアクセスが承認されたグループにユーザーを割り当てることができます。管理者は、グループに電源管理やデータバッファ管理の承認を与えることも可能です。

このマニュアルおよびソフトウェアでは、リモート認証サーバーでアカウントが設定されたユーザーをリモートユーザーと呼びます。リモートユーザーにはローカルアカウントは不要です。

Radius、TACACS+、および LDAP 認証サーバーでは、グループの設定が可能です。リモートユーザーがリモートグループのメンバーとして設定されている場合、そのユーザーの認証時には、認証サーバーからコンソールスイッチにグループ名が提示されます。コンソールスイッチにも、同じ名前のローカルグループを設定する必要があります。認証サーバーでリモートユーザーを認証したときにグループが戻されない場合、そのリモートユーザーはデフォルトで user というグループに割り当てられます。

admin グループ

admin グループのメンバーには完全な管理権限が与えられます。この権限は変更できず、デフォルトの admin ユーザーと同等のアクセス権限および設定権限です。管理者は、ポートの設定、ユーザーの追加、コンソールスイッチに接続された電源デバイスの管理を行うことができます。

メモ：admin グループに対して設定できるのは、メンバーの追加と削除だけです。

admin のアプライアンスのアクセス権を表示する

1. 「ユーザー」-「承認」-「グループ」をクリックします。「グループ」画面に、デフォルトの 4 つのユーザーグループと作成済みのすべてのグループが表示されます。

2. 「グループ」という見出しの下にある「admin」をクリックします。コンテンツ領域に「メンバー」画面が表示され、admin グループに属するすべてのメンバーが一覧表示されます。デフォルトのメンバーは admin および root ユーザーです。

メモ：「グループ名」を選択すると、コンテンツ領域とサイドナビゲーションバーが両方とも変更されます。サイドナビゲーションバーには、「メンバー」、「ログインプロファイル」および「アクセス権」（シリアル、電源、アプライアンスの権限など）に固有のメニューオプションが表示されます。

3. サイドナビゲーションバーで、「アクセス権」-「シリアル」、または「アクセス権」-「電源」をクリックすると、シリアルポートや電源の管理に関わる admin グループメンバーの固定されたアクセス権およびパーミッションを示す画面が表示されます。

メモ：「シリアル」画面および「電源」画面は読み取り専用で、変更はできません。

4. サイドナビゲーションバーで、「アクセス権」-「アプライアンス」をクリックします。「アプライアンスのアクセス権」画面に、admin グループに属するメンバーが使用できるすべてのアクセス権が表示されます。アプライアンスのアクセス権はすべて、有効の（選択された）状態で示されます。使用できるアプライアンスのアクセス権には、次のものがあります。
   - アプライアンス情報の表示
   - セッションの接続解除とアプライアンスの再起動
   - アプライアンスのフラッシュアップグレードとアプライアンスの再起動
   - アプライアンス設定の構成
   - ユーザーアカウントの構成
   - 構成のバックアップと復元
   - Shell アクセス
   - ファイルの転送

メモ：admin および appliance-admin ユーザーグループの「アプライアンスのアクセス権」画面は読み取り専用で、変更はできません。ボックスの選択を解除して「保存」をクリックすると、エラーメッセージが表示されます。コンソールスイッチではすべての権限が選択されたままになります。

appliance-admin グループ

appliance-admin グループのメンバーは、アプライアンスの管理タスクのみにアクセスが制限されています。appliance-admin ユーザーグループのメンバーは、シリアルポートや電源管理のオプションにはアクセスできません。アプライアンスのアクセス権は admin とほぼ同等ですが、「ユーザーアカウントの設定」および「シェルアクセス」は例外で、このグループでは常に無効になります。

user グループ

user グループのメンバーは、管理者が制限しないかぎりターゲットデバイスにアクセスできますが、コンソールスイッチに対するアクセス権はありません。管理者は、アプライアンスのアクセス権やパーミッションを追加するか、必要に応じてカスタムユーザー

グループにユーザーを追加して、パーミッションやアクセス権を追加できます。デフォルトでは、「アプライアンスのアクセス権」画面の選択はすべて無効になっています。

メモ：管理者はいつでも user グループの「アプライアンスのアクセス権」画面を変更できます。この変更は、コンソールスイッチの user グループの、すべてのメンバーのアクセス権に影響します。

shell-login-profile

shell-login-profile グループのメンバーは、ログイン後に shell にアクセスできます。デフォルトで、root ユーザーは、このグループに属しています。このグループは保護されておらず、削除することができます。

ユーザーグループの管理

管理者および admin グループのメンバーは、カスタムユーザーグループを作成して、いかなるユーザーも含めることができます。カスタムユーザーグループのパーミッションおよびアクセス権は、最上位レベルのユーザーグループのパーミッションによって決まります。

カスタムユーザーグループを作成する

1. 「ユーザー」-「承認」-「グループ」をクリックします。「グループ」画面に、デフォルトの 4 つのユーザーグループと追加で作成したカスタムユーザーグループが一覧表示されます。
2. コンテンツ領域で、「追加」をクリックします。
3. 新しく作成するユーザーグループの名前を入力します。
4. 「保存」をクリックします。

メンバーをユーザーグループに追加する

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. ユーザーグループの名前をクリックします。
3. 「追加」をクリックします。「メンバーの割り当て」画面が表示されます。左側のボックスに利用できるユーザーの一覧が表示され、右側のボックスは空になっています。
4. 左側の「利用できるユーザー」ボックスから右側のボックスにユーザーを移動します。ユーザー名またはグループ名をダブルクリックするか、名前を選択して「追加」ボタンをクリックすると移動できます。右側のボックスで名前をダブルクリックするか、名前を選択して「削除」ボタンをクリックすると、右側のボックスから名前を削除できます。
5. 新しいユーザーグループにリモートユーザーを追加する場合は「新規リモートユーザー」フィールドにそのユーザーを追加します。リモートの認証サーバーで有効な名前である必要があります。
6. 「保存」をクリックします。

メンバーをユーザーグループから削除する

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. ユーザーグループの名前をクリックします。
3. 削除するメンバーのボックスをチェックします。選択したメンバーを削除するために「削除」をクリックします。

ユーザーグループのログインプロファイルを設定する

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. ログインプロファイルを設定するグループの名前をクリックします。サイドナビゲーションバーの「ログインプロファイル」をクリックします。
3. 「ログインプロファイルを有効にする」チェックボックスにチェックを入れます。
4. 選択したユーザーグループがコンソールスイッチのセッションを開いた時に、ts_menu アプリケーションを使用するには「ts_menu」をクリックします。

   または

   セッションを開いた時に CLI を使用するには「CLI」を選択します。「CLI コマンド」フィールドに CLI コマンドを入力し、コマンド実行後に exit する場合は、「実行した後に終了」チェックボックスにチェックを入れます。
5. 「保存」をクリックします。

メモ：ユーザーが複数のグループに属している場合、ログインプロファイルは、グループのアルファベット順に基づいて 1 番目のログインプロファイルを有効にします。

表 3.8: ts_menu **オプション**

コマンド	**説明**
-p	TCP ポートを表示します
-i	シリアルポートに割り当てられたローカル IPv4 を表示します。
-i6	シリアルポートに割り当てられたローカル IPv6 を表示します。
-u <name>	ターゲットセッションで使用されるユーザー名
-e <[^]char>	ターゲットセッションを閉じるために使用するエスケープ文字
-l	ソート済みのポート一覧および exit
-ro	Read-Only モード
<portname>	シリアルポートへの直接接続

表 3.8: ts_menu オプション (続き)

コマンド	説明
-t	選択されたターゲットへのアイドルタイムアウト (秒単位)

ユーザーグループにシリアルポートへのアクセスを追加する

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. 新しいユーザーグループの名前をクリックします。
3. サイドナビゲーションバーで、「アクセス権」をクリックします。
4. コンテンツ領域で、「追加」をクリックします。
5. 左側の「利用可能なターゲット」ボックスから右側のボックスにシリアルターゲットデバイスを移動します。シリアルターゲット名をダブルクリックするか、ターゲットを選択して「追加」ボタンをクリックすると移動できます。右側のボックスでターゲットをダブルクリックするか、ターゲットを選択して「削除」ボタンをクリックすると、右側のボックスからターゲットを削除できます。
6. 必要なアクセス権を選択します。
7. 「保存」をクリックします。「シリアル」画面に、設定されたパーミッションを持つユーザーグループによる使用を承認した、シリアルターゲットデバイスが表示されます。
8. 必要に応じて、リスト内の 1 つ以上のターゲット名の横にあるチェックボックスを選択し、「編集」をクリックしてアクセス権を編集します。「ターゲットのアクセス権」画面にアクセス権が表示されます。必要なアクセス権を選択して「保存」をクリックします。

ユーザーグループに PDU へのアクセスを追加する

メモ : PDU へのアクセスが割り当てられたユーザーグループは、その PDU のすべての電源管理機能に対して完全なアクセス権を持ちます。ユーザーグループにコンセントへのアクセスのみを許可するには、次の「新しいカスタムユーザーグループにコンセントへのアクセスを割り当てる」の手順を実行します。

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. ユーザーグループの名前をクリックします。
3. ナビゲーションバーで、「アクセス権」-「電源」をクリックします。
4. コンテンツ領域で、「追加」をクリックします。「PDU の割り当て」画面が表示されます。左側のボックスに利用できる PDU が一覧表示されます。
5. 左側の「使用可能な PDU」ボックスから右側のボックスに PDU デバイスを移動します。PDU 名をダブルクリックするか、PDU を選択して「追加」ボタンをクリックすると移動できます。右側のボックスで PDU 名をダブルクリックするか、PDU を選択して「削除」ボタンをクリックすると、右側のボックスから PDU を削除できます。

6. 最下部のフィールドでカスタム PDU ID を指定して、カスタム PDU ID を割り当てることができます。

メモ：カスタム PDU ID は、コンソールスイッチにまだ接続されていない PDU を管理するユーザーグループ承認を割り当てるためのものです。

7. 「保存」をクリックします。

新しいカスタムユーザーグループにコンセントへのアクセスを割り当てる

メモ：ユーザーグループにコンセントへのアクセスを割り当てると、そのグループのメンバーはコンセントのオンまたはオフと、ロック機能の有効化および電源サイクル機能を PDU 上で実行できるようになります。

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. 新しいユーザーグループの名前をクリックします。
3. ナビゲーションバーで、「アクセス権」-「電源」-「コンセント」をクリックします。
4. 「追加」をクリックします。「電源」画面が表示されます。
5. 接続済みの PDU の場合、「PDU の選択」ボタンをクリックすると、「接続されている PDU」および「コンセント」フィールドがアクティブになります。
6. プルダウンメニューから「接続されている PDU」を選択します。
7. ユーザーグループに割り当てるコンセントを入力します。

メモ：コンセントは個別に指定できます。たとえば、1,3,6,8 のようにコンマで区切るか、1-4 のように範囲で指定するか、1-4,6,8 (1、2、3、4、6、および 8 のコンセントへのアクセスを割り当て) のように両方を組み合わせた形で指定できます。

8. 将来使用するためにカスタム PDU ID を作成して、コンセントをあらかじめ割り当てておく場合は、「カスタム」ボタンをクリックし、カスタム PDU ID 名を入力してコンセントを指定します。
9. 「保存」をクリックします。

カスタムユーザーグループにアプライアンスのアクセス権を割り当てる

1. 「ユーザー」-「承認」-「グループ」をクリックします。
2. 新しいユーザーグループの名前をクリックします。
3. ナビゲーションバーで、「アクセス権」-「アプライアンス」をクリックします。
4. 必要なアプライアンスのアクセス権を選択して「保存」をクリックします。

イベント通知

コンソールスイッチでは、さまざまなイベントに関する通知が生成されます。コンソールスイッチでイベント通知を設定し、さまざまな宛先へ直接送信してすぐに利用できるようにすることも、あとで分析するために保存しておくこともできます。

イベントリスト

「イベントリスト」画面には、SNMP トラップ、Syslog、MergePoint Access、電子メール、および SMS 用に各々設定されたコンソールスイッチイベントが一覧表示されます。

イベントを設定する

1. 「イベントとログ」-「イベントリスト」をクリックします。
2. 通知を送信するイベントを探し、イベント番号の横にあるチェックボックスを 1 つ以上選択します。
3. 「編集」をクリックします。
4. 設定したタイプのイベント送信先にイベント通知を送信する場合、関連する「送信」チェックボックスをクリックします。
5. 「保存」をクリックします。「イベント」ページが表示されます。「イベント設定」画面で「送信」ボックスをチェックしていると、その送信先タイプの下の列に「V」と表示されます。

イベントの送信先

コンソールスイッチは、幅広いイベント通知を生成します。コンソールスイッチを設定して、即時使用するために直接イベント通知する、あるいは、後で分析するために、様々な送信先にイベント通知を保存することができます。

イベントの送信先の設定

1. 「イベントとログ」-「イベントの送信先」をクリックします。
2. 「イベントとログ」-「イベントの送信先」をクリックします。
3. 「リモートサーバー – IPv4」を選択し、IPv4 アドレスまたはホスト名を入力すると、1 つ以上のリモートの IPv4 syslog サーバーへの syslog メッセージ送信が有効になります。コンマによって複数のサーバーアドレスをセパレートします。

   または

   「リモートサーバー – IPv6」を選択し、IPv6 アドレスまたはホスト名を入力すると、1 つ以上のリモートの IPv6 syslog サーバーへの syslog メッセージ送信が有効になります。コンマによって複数のサーバーアドレスをセパレートします。
4. 「アプライアンスコンソール」を選択すると、コンソールスイッチの CONSOLE へのメッセージが送信されます。
5. 「root セッション」を選択すると、root ユーザーとしてログインしたすべてのセッションに対して syslog メッセージが送信されます。
6. SNMP トラップ項目で、「コミュニティ」フィールドに 1 つ以上の SNMP トラップサーバーにおいて定義されたコミュニティ名を入力し、その後「サーバー」フィールドに 5 つまでのサーバーの IP アドレスを入力します。

7. SMS 項目で、適切なフィールドに SMS サーバー、ポート、および ポケットベル番号の情報を入力します。
8. 電子メール項目で、適切なフィールドにサーバー、ポート、送信先電子メールの情報を入力します。
9. MergePoint Access 項目で、「MergePoint Access サーバー」フィールドにイベント通知を送信する MergePoint Access サーバーの IP アドレスを入力します。適切なフィールドに MergePoint Access サーバー用の syslog サーバーポート番号、SSH 情報、およびバッファー警告情報を入力します。
10. 「保存」をクリックします。

データバッファ

データバッファを設定する

1. 「イベントとログ」-「データバッファ」を選択します。
2. 「ローカル用データバッファ設定」セクションで「セグメントサイズ」をキロバイト単位で入力し、「予備セグメント」も入力します。
3. 「NFS 用データバッファ設定」セクションで、「NFS サーバー」、「NFS パス」、「セグメントサイズ (キロバイト)」、および「予備セグメント」を入力します。

メモ：「NFS 用データバッファ設定」を設定する前に、「セキュリティプロファイル」画面で RPC サービスを有効にする必要があります。NFS は IPv6 をサポートしていません。

4. 「Syslog データバッファ設定」セクションで、Syslog サーバーのデータバッファストレージを設定します。ドロップダウンメニューの「Log Local 0」、「Log Local 1」、「Log Local 2」、「Log Local 3」、「Log Local 4」、および「Log Local 5」からファシリティ番号を選択します。
5. 「保存」をクリックします。

アプライアンスログ

アプライアンスログを設定する

1. 「アプライアンス セッション データ ログを有効にする」をクリックします。
   a. プルダウンメニューからアプライアンスセッションデータログの送信先を選択します。「ローカル」、「NFS」、「Syslog」、「MergePoint Access」から選択できます。
   b. アプライアンスセッションデータログのタイムスタンプを有効、または 無効にします。
2. 「アプライアンス セッションのデータログ アラートを有効にする」をクリックします。
3. 提示されたフィールドに必要なアラートストリングを入力します。ストリングは最大 10 件指定できます。
4. 「保存」をクリックします。

センサー

コンソールスイッチには、内部の温度を監視するセンサーがあります。コンソールスイッチの動作範囲を環境に合わせて指定できます。

注意：65 ページの「技術仕様」の一覧に示す最高温度と最低温度の範囲外の値を使用しないでください。

温度センサーを設定する

1. 「イベントとログ」-「センサー」をクリックします。
2. 「最高検出温度」フィールドに温度を摂氏で入力します。この温度を超えると、イベント通知が生成されます。
3. 「温度の最大しきい値」フィールドに、最高検出温度よりも低い温度のしきい値を摂氏で入力します。

メモ：温度の最大しきい値は、最高検出温度のまわりの範囲に定義します。温度が「最高検出温度」に「温度の最大しきい値」を加えた温度を超えるとイベント通知が生成されます。「最高検出温度」からこのしきい値を引いた温度を下回ると、コンソールスイッチが正常な動作温度に戻ったことを知らせるイベント通知が生成されます。これは「温度の最小しきい値」の設定についても同様です。

---

4. 「最低温度」フィールドに温度を摂氏で入力します。コンソールスイッチの温度が、この値を下回るとイベント通知が生成されます。
5. 「温度の最小しきい値」フィールドに、最低温度よりも高い温度のしきい値を摂氏で入力します。
6. 「保存」をクリックします。

電源管理

接続された電源デバイスを、電源のリモート管理に使用できます。電源管理が承認されているユーザーは、コンソールスイッチから、接続状態の PDU に接続されているデバイスの電源をオンまたはオフにしたり、デバイスをリセットしたりできます。

次の PDU は任意のシリアルポートまたは AUX ポートに接続できます。

- FW-SPM230
- FW-SPM115
- FW-SPM130

PDU

PDU を管理する

1. 「電源管理」-「PDU」を選択します。
2. 電源を管理する PDU の横にあるチェックボックスを選択します。
3. 必要に応じて 「オフ」、「オン」、「電源オフ / オン」、「PDU を再起動する」あるいは、「デフォルト設定」をクリックします。確認表示されます。「OK」をクリックします。

メモ：電源制御（オフ、オン、電源オフ / オン）は、PDU のすべてのコンセントに適用されます。

4. PDU ID を変更するには、「名前の変更」をクリックし、「新規 PDU ID」フィールドに名前を入力します。
5. 「保存」をクリックします。

PDU の情報を表示する

1. 「電源管理」-「PDU」を選択します。
2. 表示あるいは管理する PDU の名前をクリックします。
3. 電源制御ウィンドウにコンセントテーブルが表示され、サイドナビゲーションバーにオプションの一覧が表示されます。
4. PDU のコンセントを表示するには、
   a. 管理するコンセント番号のチェックボックスにチェックを入れます。
   b. 選択したコンセントの機能を実行するために、「オン」、「オフ」、「電源オフ / オン」、「ロック」、あるいは「ロック解除」をクリックします。
5. PDU の情報を表示するために、サイドナビゲーションバーで「情報」をクリックします。
6. 適切な情報のテーブルを表示するために、サイドナビゲーションバーで「電流」、「電圧」、「消費電力」、「累積電力」、あるいは「環境」をクリックします。最大、最小、および平均値をクリアするために、「値のリセット」をクリックします。

ファームウェアをアップグレードする

1. サイドナビゲーションバーで「概要」をクリックし、「ファームウェアのアップグレード」をクリックします。
2. すべてのフィールドに正しい情報を記入し、コンソールスイッチにファームウェアをダウンロードするために「ダウンロード」をクリックします。
3. ダウンロードが完了すると、PDU ファームウェアのインストール画面が表示されます。バージョン情報が正しければ、「アップグレードを実行」をクリックして、PDU のファームウェアアップグレードを開始します。
4. アップグレードが完了すると、アップグレード操作の結果がアップグレードの完了画面に表示されます。

PDU のコンセントを管理する

1. サイドナビゲーションバーを拡張するために、「設定」をクリックします。
2. 「コンセント」をクリックします。
3. 設定を変更するコンセント番号をクリックします。「名前」および「POST オンの遅延」変更し、「保存」をクリックして、「閉じる」をクリックします。

   あるいは

設定を変更するコンセントの横にある 2 つ以上のチェックボックスにチェックを入れます。「編集」をクリックします。「プレフィックス名」（コンセント名は、プレフィックス名＋サフィックスとなります。) および POST オンの遅延を変更します。「保存」をクリックします。

4. 「PDU」をクリックすると、PDU の設定を確認できます。「公称電圧」、「推定力率」、「電流のエラーのしきい値」を変更します。完了したら、「保存」をクリックします。
5. 「バンク」をクリックします。
   a. 設定を変更するバンクの名前をクリックする、あるいは変更するバンクの横にある 1 つ以上のチェックボックスをクリックします。「電流エラーのしきい値」変更します。
   b. 「保存」をクリックして、設定を保存し、「閉じる」をクリックしてバンク画面に戻ります。

メモ：PDU モデルでは、使用できるパラメーターを「設定」ウィンドウで定義します。

ログイン

管理者は、サポートしている PDU タイプのログインパスワードを変更することができます。このパスワードは、コンソールスイッチで PDU と通信する際に使用されます。（パスワードは、同じタイプのすべての PDU に対して 1 つだけサポートされます。）

PDU パスワードを変更する

1. 「電源管理」-「ログイン」を選択します。
2. パスワードを変更するには、「パスワード」フィールドにパスワードを入力します。
3. 「保存」をクリックします。

メモ：新規パスワードは、検出されたすべての PDU に適用されます。

コンセントグループ

「コンセントグループ」タブを選択すると、設定はもちろん、そのグループに属しているコンセントグループの状態およびコンセントを参照できます。選択したコンセントグループのオン、オフ、オフ / オンも可能です。

コンセントグループを管理する

1. 「電源管理」-「コンセントグループ」を選択します。
2. 管理するコンセントグループの名前の横にあるボックスをチェックします。
3. 必要に応じて、「オン」、「オフ」、または「電源のオフ / オン」ボタンをクリックします。

   あるいは

4. 「追加」ボタンをクリックして、コンセントグループを追加します。コンセントグループ画面が表示されます。「グループ名」フィールドに名前を追加します。
5. 「保存」をクリックします。

コンセントグループの情報を表示して変更する

1. 「電源管理」-「コンセントグループ」を選択します。
2. 情報を表示する、あるいは管理するコンセントグループの名前をクリックします。
3. コンセントを追加するには、「追加」をクリックし、グループに新規コンセントを追加します。フィールドに記入し、「保存」をクリックすると「コンセントグループの詳細」テーブルに戻ります。
4. コンセントを削除するには、グループから取り除くコンセントの横にあるボックスにチェックします。「削除」をクリックし、完了したら、「閉じる」をクリックします。

アクティブセッション

コンソールスイッチでは、複数のユーザーが同時にログインしてセッションを実行できます。アクティブセッション機能を利用すると、アクティブセッションをすべて参照して不要なセッションを終了（中止）できます。「アクティブセッション」をクリックすると、コンソールスイッチで開いているすべてのセッションを参照できます。

メモ：この画面の表示中にコンソールスイッチで別のセッションを開始した場合、そのセッションは Web マネージャウィンドウの最上部にある「更新」をクリックするまで表示されません。

アクティブセッションを中止する

1. 「アクティブセッション」をクリックします。「アクティブセッション」画面に、ユーザーのワークステーションの IP 別に、コンソールスイッチに対して開いているすべてのセッションが一覧表示されます。
2. 中止するセッションの横にあるチェックボックスを選択し、「中止」ボタンをクリックします。数秒後、「アクティブセッション」画面に開いているセッションがふたたび表示され、中止したセッションが削除されたことを確認できます。

監視

「監視」をクリックすると、ネットワークやシリアル状態などのさまざまな情報を参照できます。この画面は参照専用で、ユーザーが対話式に操作することはできません。参照できる情報のタイプを次の表に示します。

表 3.9: 監視画面

画面名	定義
「ネットワーク」-「デバイス」	Ethernet ポート、PC カードデバイス名、状態 (有効または無効)、IPv4 アドレス、IPv4 マスク、および IPv6 アドレスが表示されます。
「ネットワーク」-「IPv4 経路表」	送信先、ゲートウェイ、Genmask、フラグ、メトリック、Ref、使用、および Iface が表示されます。
「ネットワーク」-「IPv6 経路表」	送信先、次のホップ、フラグ、メトリック、**Ref**、使用、および Iface が表示されます。
「シリアルポート」	デバイス名、プロファイル、設定、信号、Tx バイト、Rx バイト、フレームエラー、パリティエラー、ブレーク、およびオーバーランが表示されます。

パスワードの変更

管理者およびユーザーは、この画面から自分自身のパスワードを変更できます。

自分自身のパスワードを変更する

1. 「パスワードの変更」を選択します。
2. 元のパスワードおよび新しいパスワードを適切なフィールドに入力します。
3. 「パスワードの確認」フィールドに新しいパスワードを入力し、「保存」をクリックします。

一般ユーザー向けの Web マネージャの概要

次の図は、一般ユーザー向けの Web マネージャの機能を示しています。
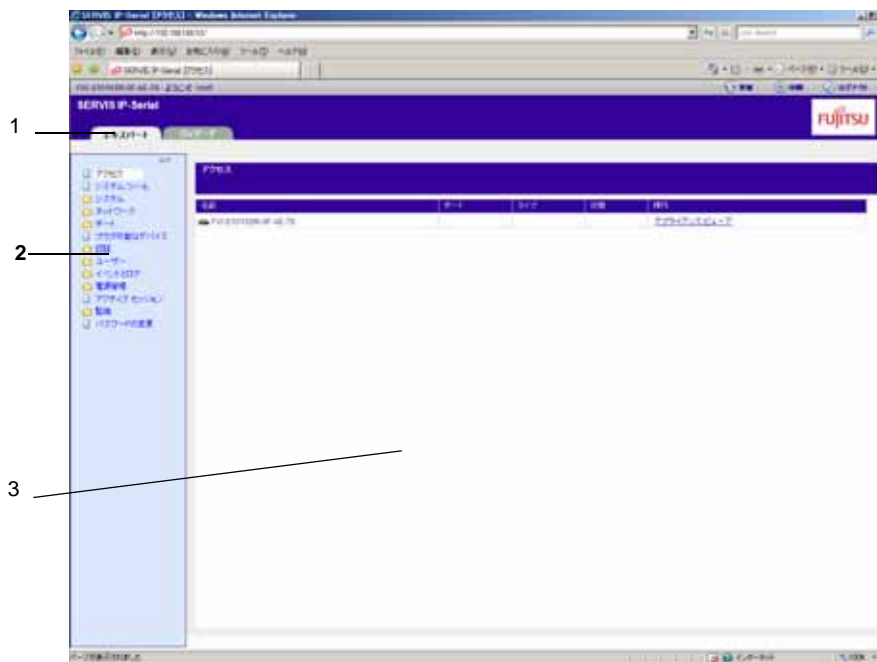
図 3.3: **一般ユーザー向けの** Web **マネージャの画面**

表 3.10: **一般ユーザー向けの** Web **マネージャ画面の各部**

番号	説明
1	最上部のオプションバー。左側にはアプライアンス名、ログインしたユーザー名、右側には「更新」、「印刷」、「ログアウト」ボタンが表示されます。
2	サイドナビゲーションバー。一般ユーザーが使用できるメニューオプションが表示されます。
3	コンテンツ領域。内容はサイドナビゲーションバーで選択したオプションによって異なります。

次の表に、一般ユーザー向けのオプションの概要を示します。

表 3.11: 一般ユーザー向けの Web マネージャオプション

メニューオプション	説明
アクセス	ユーザーがアクセスすることができるすべてのデバイスが表示されます。そのデバイスのターミナルセッションを開始するには、デバイスの操作列の「シリアルビューア」をクリックします。
電源管理 • PDU • コンセントグループ	• 「PDU」をクリックし、コンソールスイッチに接続された PDU の電源オン、電源オフ、電源オフ / オン、再起動、デフォルト設定に戻す、あるいは、名前の変更を行います。 • 「コンセントグループ」をクリックし、PDU に接続されたコンセントのグループ管理を行います。
パスワードの変更	自分自身のパスワードを変更します。

付録

付録 A: 技術仕様

表 A.1: コンソールスイッチハードウェアの技術資料

一般情報	
CPU	PPC440EPx @ 533 MHz (SAE (Security Acceleration Engine) 搭載 PowerPC)
メモリ	256 MB DDR-2 / 128 MB NAND フラッシュ (マザーボード上の内蔵 IC)
インターフェイス	2 Ethernet 10/100/1000BT on RJ-45 1 RS232 コンソール x1 (RJ-45) 1 AUX RS232 x1 (RJ-45) RS232 シリアルポート x1 (RJ-45) 1 USB 2.0 ホスト x1 (A タイプコネクタ) 2 PC カード / CardBus (イジェクタ付き)x2 (デュアル Type II またはシングル Type III)
電源情報	
電源装置	内部 100-240 VAC, 50/60 Hz
消費電力	公称電圧 120 VAC: 通常 0.17 A, 20 W 最大 0.25 A, 30 W 公称電圧 230 VAC: 通常 0.1 A, 23 W 最大 0.15 A, 35 W
周囲空気条件	
動作時の温度	0º C ～ 50º C (32 ºF ～ 122 ºF)
保管時の温度	-20º C ～ 70º C (-4 ºF ～ 158 ºF)
湿度	相対温度 20% ～ 80% (結露なし) 動作時温度の全範囲に適用
寸法	
高さ x 幅 x 奥行	4.3561 x 43.815 x 24.13 cm (1.715 x 17.250 x 9.50 インチ)
重量	2.994 kg (6.6 ポンド)

表 A.1: コンソールスイッチハードウェアの技術資料 (続き)

認定	電磁環境適合性 : FCC Class A (北米)、CE Class A (欧州)、ICES-003 (カナダ)、VCCI-A (日本)、C-Tick (オーストラリア、内部モデムなし)、GOST (ロシア)、KCC/RRL (韓国) 安全性 : UL 60950-1 (北米)、cUL (カナダ)、CE マーク、CB、GS

付録 B: コンソールスイッチのパスワードの復元

コンソールスイッチの root パスワードを復元する

1. コンソールスイッチの CONSOLE ポートに直接接続します。
2. コンソールスイッチの電源をオフし、その後、再びオンします。
3. uboot プロンプトにアクセスするためにスペースキーを入力します。.
4. **hw_boot single** と入力し、エンターキーを押下します。
5. コンソールスイッチは、シングルユーザーモードで起動します。**passwd** と入力し、エンターキーを押下します .
6. 新しいパスワードおよびパスワード確認
7. **reboot** と入力しコンソールスイッチを通常起動させます。

付録 C: ダイヤルアップ経由で MergePoint Access ソフトウェア認定されたコンソールスイッチにアクセスする

MergePoint Access ソフトウェアユーザーがシリアルセッションを確立する場合、次のようなイベントが発生します。

- ユーザーがシリアルポートへのアクセスを選択します。
- ビューアが MergePoint Access サーバーからユーザーのワークステーションにダウンロードされます。
- MergePoint Access ソフトウェアがビューアへ情報を渡します。情報とは、認証キー、コンソールスイッチの IP アドレス、およびシリアルポートなどです。
- その後、ビューアは、MergePoint Access サーバーから取得した認証キーを送信することによって、SSH セッション経由でコンソールスイッチのシリアルポートへアクセスします。
- シリアルセッションが開始します。

MergePoint Access サーバーは、帯域外 (OOB) バックドアに設定することが出来ます。それは、ネットワークあるいはインターネット障害のイベントにおいて、モデム経由でコンソールスイッチにアクセスすることが許可されます。

OBB バックドアを持つ MergePoint Access ソフトウェアの設定

MergePoint Access サーバーは、モデムが接続されたハードウェア上で動作します。コンソールスイッチは、PCMCIA カード、USB、あるいはシリアルポート経由でモデムにアクセスされます。

この設置において、MergePoint Access サーバーは、ダウンロードされたビューアおよびコンソールスイッチの間のパケット受信の中心点になります。これを保証するために、プロキシモードが MergePoint Access ソフトウェアの範囲内に設定されます。その後、ビューアは、SSH 接続を確立するために MergePoint Access サーバーを指し示します。その後、MergePoint Access サーバーは、ソースおよび送信先 IP アドレスの両方の変更により、パケットが送信され、通信の中間点として動作します。

正常動作状態において、ビデオビューアから受信したパケットは、Ethernet 経由で MergePoint Access サーバーへ送信されます。エラー状態において、MergePoint Access サーバーは、割り込みでコンソールスイッチへの正常パスを検出し、コンソールスイッチへのダイヤルアウト、認証の送信、PPP 接続の確立を行います。Ethernet 経由で正常送信されたパケットは、代わりに PPP 経由で送信されます。

Ethernet とダイヤルアップの間の速度の違いのために、性能は今のところ、顕著に低下します。複数のユーザーの接続では、さらに性能は低下しますので、お勧めできません。このため、ダイヤルアップバックアップは、緊急バックアップ機能としてのみ推奨します。

コンソールスイッチのダイヤルアップ設定

MergePoint Access ソフトウェア内のコンソールスイッチへのダイヤルアップ設定を行う

1. アプライアンスを含むユニットビューウィンドウにおいて、設定を行うコンソールスイッチを選択します。コールバックでのダイヤルインのためには、まず、システムタブにおいて、「MergePoint Access サーバー」-「プロパティ」-「MergePoint Access モデムセッション」を選択し、「アナログ電話番号」フィールドに MergePoint Access サーバーに割り当てられた電話番号を入力します。
2. 「MergePoint Access 設定」-「ダイヤルアップ」を選択します。
3. 「モデムタイプ」-「アナログ」を選択します。
4. 使用するコンソールスイッチの電話番号を入力します。
5. 適切なフィールドに「PPP ユーザー」を入力し、「PPP 認証プロトコル」を選択します。
6. コールバックでのダイヤルインのために、ダイヤルバックチェックボックスを有効にします。
7. 「MergePoint Access 設定」-「ダイヤルアップ」-「PPP パスワード」を選択し、その後コンソールスイッチにアクセスするためのパスワードおよびパスワードの確認を入力します。
8. 「MergePoint Access 設定」-「ダイヤルアップ」-「IP アドレス」を選択します。
9. 自動的に IP アドレスを設定するために、「自動生成」をクリックする、あるいは手動で「PPP ローカル IP アドレス」および「アプライアンス IP アドレス」を入力します。

MergePoint Access ソフトウェア内のダイヤルアップ接続を受信するためにコンソールスイッチを設定する

1. アプライアンスを含むユニットビューウィンドウにおいて、設定を行うコンソールスイッチを選択します。
2. シリアルポートに接続されたモデムのために、「ポート」-「シリアルポート」を選択します。その後、接続されたモデムを含むポートを選択します。

   あるいは

   補助ポートに接続されたモデムのために、「ポート」-「補助ポート」を選択します。その後、ポートを選択します。「ダイヤルイン設定」をクリックします。

   あるいは

   プラグ可能なデバイスのモデムのために、「プラグ可能なデバイス」を選択し、モデムを選択します。

3. コールバックでのダイヤルインのために、「ポート」-「ダイヤルインプロファイル」-「デバイス」を選択し、ダイヤルインに使用するモデムを選択します。

   あるいは

   ワンタイムパスワード（OTP）でのダイヤルインのために、「ポート」-「ダイヤルインプロファイル」-「セキュアダイヤルイン」-「設定」をクリックし、「アプライアンスへのログイン」フィールドの横にある「有効にする」を選択します。
4. 「PPP アドレス」フィールドにおいて、「リモートピアからの構成を許可する」を選択します。
5. 「PPP 認証」フィールドにおいて、「アプライアンス」を選択し、プロトコルを設定します。

   あるいは

   コールバックでのダイヤルインのために、「PPP 認証」フィールドにおいて、「リモートピア」を選択し、プロトコルを設定します。
6. 「ポート」-「ダイヤルインプロファイル」-「設定」をクリックし、「アプライアンスへのログイン」フィールドにおいて、「無効にする」を選択します。（PPP 以外にもターミナルアクセスさせる場合は、「有効にする」を選択します。あるいは、コールバックによってのみターミナルアクセスさせたい場合、「コールバック」を選択します。）

   あるいは

   OTP でのダイヤルインのために、「ポート」-「ダイヤルインプロファイル」-「設定」をクリックし、コンソールスイッチに OTP ではない接続を受信させたい場合、「有効にする」を選択します。
7. 「OTP ログイン認証」フィールドにおいて、「無効にする」を選択します。

   あるいは

   OTP でのダイヤルインのために、「OTP ログイン認証」フィールドにおいて、「有効にする」を選択します。
8. 「PPP 接続」フィールドにおいて、「有効にする」を選択します。

   あるいは

   OTP でのダイヤルインのために、コンソールスイッチに OTP ではない接続を受信させたい場合、「無効にする」を選択します。
9. 「PPP/PAP 認証」フィールドにおいて、「ローカル」を選択します。
10. OTP でのダイヤルインのために、「ポート」-「ダイヤルインプロファイル」-「コールバックユーザー」をクリックし、適切なフィールドに PPP ユーザーおよびコールバック番号を追加します。

    あるいは

OTP でのダイヤルインのために、「ポート」-「ダイヤルインプロファイル」-「セキュアダイヤルイン」-「PPP」-「OTP ユーザー」をクリックし、OTP ユーザーを追加します。

11. 「ユーザー」-「ローカルアカウント」-「ユーザー名」をクリックし、適切なフィールドに「PPP ユーザー」および「パスワード」を追加します。

メモ：MergePoint Access ソフトウェア設定ダイヤルアップウィンドウの「PPP 認証プロトコル」フィールドにおいて、「CHAP」が選択されている場合、次のステップのみが必要となります。

---

12. コンソールスイッチの CLI にログインし、Linux シェルにアクセスします。/etc/ppp/chap-secrets を編集し、その書式で行を追加します。第 1 列は、PPP ユーザーであり、第 3 列は、次の例に示すように PPP パスワードです。

```
pppuser              *              "ppppassword"              *
```

付録 D: 安全性、規制、および法令遵守の情報

この付録には、コンソールスイッチの安全性、規制、および法令遵守に関する情報を記載します。

コンソールスイッチのラック搭載に関する安全性および環境のガイドライン

コンソールスイッチをラックに搭載する場合は、次の事項について考慮する必要があります。

温度

メーカー推奨のコンソールスイッチの最高周囲温度は 50 ºC (122 ºF) です。

動作時の周囲温度の上昇

コンソールスイッチを密閉式またはマルチユニットのラックアセンブリに設置した場合、動作時のラック環境の周囲温度が室内の周囲温度より高くなる可能性があります。そのため、メーカーが指定する最高定格周囲温度に適合した環境に装置を設置するよう考慮する必要があります。前項を参照してください。

通気の不足

装置をラックに設置する際は、装置の安全な動作に必要な通気が妨げられないようにしてください。

機械的負荷

装置をラックに設置する際は、不均等な機械的負荷によって危険な状態が生じないように設置する必要があります。

回路の過負荷

装置の電源回路への接続に考慮して、回路の過負荷が過電流保護および電源の配線に与える影響に注意してください。対処方法として、装置のネームプレートに記載された定格を適切に考慮してください。

確実な接地

ラックに搭載した装置の確実な接地を維持してください。分岐回路への直接接続のほか、電源コードや延長コードなどの給電接続にも特別な注意をする必要があります。

コンソールスイッチを使用する際の安全措置

ユーザーとコンソールスイッチの保護のため、次の安全性ガイドラインをすべてお読みください。

警告：カバーを取り外したままでコンソールスイッチを使用しないでください。

注意：ネットワークケーブルを取り外す際は、コンソールスイッチのショートを防ぐため、まずホストサーバーからケーブルを外し、装置から外部電源を外したうえで (該当する場合)、ネットワークの差込口からケーブルを外します。装置の背面にネットワークケーブルを再接続する際は、まずネットワークの差込口にケーブルを差し込み、次にホストサーバー装置に差し込みます。

注意：感電を防ぐため、コンソールスイッチは適切に接地された電源に接続してください。適切な接地ができるよう、ケーブルには 3 ピンのプラグが付いています。アダプタープラグを使用したり、ケーブルからアースピンを外したりしないでください。延長ケーブルを使用する必要がある場合は、適切に接地されたプラグの付いた三線ケーブルを使用してください。

注意：コンソールスイッチを電力の変動から保護するため、サージ抑制器、ラインコンディショナー、または無停電電源装置を使用してください。コンソールスイッチのケーブル上に何も載っていないこと、また、人が踏んだり、つまずいたりする可能性のある場所に設置されていないことを確認してください。コンソールスイッチの上に食品や液体をこぼさないでください。

注意：コンソールスイッチの開口部に物を押し込まないでください。物を押し込むと内部コンポーネントがショートし、火災や感電が起こることがあります。

注意：コンソールスイッチは熱源から遠ざけて設置してください。また、ホストの冷却用通気孔をふさがないでください。

注意：火災の危険性を軽減するために、No. 26 AWG またはそれ以上の UL または CSA 認定された通信線コード (24 AWG など) のみを使用してください。

コンソールスイッチ内部の操作

技術サポートの担当者から指示されないかぎり、コンソールスイッチの保守をユーザー自身で行わないでください。技術サポートからの指示により作業する場合は、まず、次の注意事項に従います。

- コンソールスイッチのスイッチを切ります。
- ユニットの内部に触れる前に、装置の背面にある未塗装の金属面に触れて感電を防ぎます。

メモ：FCC 標準に準拠するため、コンソールスイッチを使用する際は、すべてのポート接続に CAT5 のシールドケーブルを使用する必要があります。このケーブルは製品には付属していないため、お客様側で準備していただく必要があります。表紙裏の「FCC 警告」および「カナダ DOC 通知」を参照してください。

静電放電 (ESD) の安全措置

電子部品または組み立て部品を扱う際は、次の静電気防止対策を実施して破損を防ぐ必要があります。

- プリント基板周辺の作業をする際は、接地されたリストストラップを必ず着用してください。
- すべての組み立て部品、コンポーネント、およびインターフェイスの接続を、静電気に弱いものとして取り扱ってください。
- カーペットをひいた場所での作業は避けてください。
- 基板の取り外しまたは取り付けの際は、静電気の蓄積を最小にするため、本体はできるだけ動かさないようにしてください。

バッテリーの交換

注意：バッテリーの交換を不適切に行うと爆発する危険性があります。メーカーが推奨するバッテリー、または同等のバッテリーのみを使用してください。使用済みのバッテリーは、メーカーの指示に従って破棄してください。

付録 E: 技術サポート

問題が発生した場合は、次の手順に従って、できるだけ早急に保守を行なってください。

問題を解決する

1. このマニュアルの該当する項目を参照し、説明されている手順を実行して問題を解決できるかどうかを確認します。
2. servis-center@fcl.fujitsu.com に電子メールを送り、技術サポートに問い合わせます。